Betriebsanleitung
00809-0205-4420, Rev GA
April 2013

Smart Wireless Gateway



ROSEMOUNT

EMERSON
Process Management

Smart Wireless Gateway

HINWEIS

Lesen Sie diese Betriebsanleitung, bevor Sie mit dem Produkt arbeiten. Bevor Sie das Produkt installieren, in Betrieb nehmen oder warten, sollten Sie über ein entsprechendes Produktwissen verfügen, um somit eine optimale Produktleistung zu erzielen sowie die Sicherheit von Personen und Anlagen zu gewährleisten.

Emerson Process Management verfügt innerhalb der USA über zwei gebührenfreie Kundendienstnummern:

Global Service Center
Unterstützung Software und Integration

1-800-833-8314 (USA)

+63-2-702-1111 (International)

Kundendienst
Technischer Kundendienst, Angebote und Fragen zu Aufträgen.

1-800-999-9307 (7.00 bis 19.00 Uhr CST)

Response Center Nordamerika
Geräteservice

1-800-654-7768 (24 Stunden – inkl. Kanada)

Außerhalb der USA wenden Sie sich bitte an Emerson Process Management.

⚠ WARNUNG

Die in diesem Dokument beschriebenen Produkte sind NICHT für nukleare Anwendungen qualifiziert und konstruiert. Werden Produkte oder Hardware, die nicht für nukleare Anwendungen qualifiziert sind, im nuklearen Bereich eingesetzt, kann das zu ungenauen Messungen führen.

Informationen zu nuklear-qualifizierten Rosemount Produkten erhalten Sie von Emerson Process Management.

Inhalt

Abschnitt 4: Einrichtung der Software

Abschnitt 5: Host-Integration

Abschnitt 6: Störungsanalyse und -beseitigung

Abschnitt 7: Glossar

Anhang A: Technische Daten

Anhang B: Produkt-Zulassungen

Anhang C: Delta V Ready

Anhang D: Redundanz

Abschnitt 1 Übersicht

1.1 Sicherheitshinweise

Die in dieser Betriebsanleitung beschriebenen Vorgehensweisen und Verfahren können besondere Vorsichtsmaßnahmen erforderlich machen, um die Sicherheit des Bedienpersonals zu gewährleisten. Informationen, die eine erhöhte Sicherheit erfordern, sind mit einem Warnsymbol (⚠) gekennzeichnet. Vor Durchführung von Verfahren, die mit diesem Symbol gekennzeichnet sind, diese Sicherheitshinweise beachten.

⚠ WARNUNG

Nichtbeachtung dieser Installationsrichtlinien kann zu schweren oder tödlichen Verletzungen führen.

- Die Installation darf nur von Fachpersonal durchgeführt werden.

Explosionen können zu schweren oder tödlichen Verletzungen führen.

- Sicherstellen, dass die Prozessatmosphäre des Geräts den entsprechenden Ex-Zulassungen entspricht.

Elektrische Schläge können zu schweren oder tödlichen Verletzungen führen.

- Bei Kontakt mit Leitungen und Anschlüssen äußerst vorsichtig vorgehen.

1.2 Einleitung

Das Smart Wireless Gateway verbindet selbstorganisierende WirelessHART™ Netzwerke mit Hostsystemen und Datenanwendungen. Die universelle Integration und Systeminteroperabilität wird durch Modbus Kommunikation über RS-485 oder Ethernet gewährleistet. Die optionale OPC Funktionalität des Gateway bietet eine Möglichkeit, an neuere Systeme und Anwendungen anzubinden und gleichzeitig umfangreichere Daten bereitzustellen.

Das Smart Wireless Gateway bietet industrieführende Sicherheit, Skalierbarkeit und Datenzuverlässigkeit. Layered Security gewährleistet die Sicherheit des Netzwerks. Zusätzliche Geräte können jederzeit hinzugefügt werden. Durch die automatische Verwaltung des Netzwerks durch das Gateway besteht keine Notwendigkeit, die Kommunikationswege zu konfigurieren. Dieses Merkmal gewährleistet außerdem, dass die Daten der WirelessHART Feldgeräte auf dem zuverlässigsten Weg gesendet werden.

Lieferumfang

Im Lieferumfang des Smart Wireless Gateway sind verschiedene Teile enthalten, die für die Installation und den Betrieb des Gateway erforderlich sind.

- Smart Wireless Gateway
- Kurzanleitung
- Softwarepaket mit 2 CDs
- Befestigungsteile
- Verschlussstopfen, 4 Stück
- Leitungseinführungsadapter (optional)

Bei Bestellung einer optionalen externen Antenne werden die folgenden Teile separat geliefert:

- Antenne für externe Montage
- Befestigungsteile
- Überspannungsschutz
- Kabel (1 oder 2 Stück mit insgesamt 15,2 m [50 ft.] Länge)
- Koaxialkabel-Abdichtband

1.3 Betriebsanleitung

Diese Betriebsanleitung enthält die erforderlichen Anweisungen für die Installation, Konfiguration, Bedienung und Wartung des Gateway.

Abschnitt 1 – Übersicht

Dieser Abschnitt ist eine Produkteinführung und eine Beschreibung der im Lieferumfang enthaltenen Komponenten. Außerdem sind in diesem Abschnitt Einzelheiten zum Service und Support sowie zur Rücksendung und Entsorgung des Produkts zu finden.

Abschnitt 2 – Erstanschluss

Dieser Abschnitt enthält Anweisungen für den erstmaligen Anschluss des Gateway und die zu konfigurierenden Einstellungen, bevor das Gateway mit einem aktiven Leitnetzwerk verbunden wird. Dabei ist zu beachten, dass manche Gateways in eigenständigen Anwendungen verwendet werden und kein Teil eines Netzwerks sind. In diesen Fällen müssen die in diesem Abschnitt aufgeführten Konfigurationseinstellungen jedoch ebenfalls durchgeführt werden.

Abschnitt 3 – Montage und Anschluss

Dieser Abschnitt enthält Anweisungen für die ordnungsgemäße Montage des Gateway und den elektrischen Anschluss, einschließlich der elektrischen Verdrahtung, Erdung und Anschlüsse des Hostsystems. Außerdem sind in diesem Abschnitt Anweisungen zur Montage der optionalen externen Antenne zu finden.

Abschnitt 4 – Einrichtung der Software

Dieser Abschnitt enthält Anweisungen für die Installation und Einrichtung der optionalen Software, die im Lieferumfang des Smart Wireless Gateway enthalten ist. Diese Software erleichtert die Integration in ein sicheres Hostsystem sowie die Konfiguration von Wireless Feldgeräten.

Abschnitt 5 – Host-Integration

Dieser Abschnitt enthält Anweisungen für die Verbindung des Gateway mit einem Hostsystem und die Integration der vom Feldgerätenetzwerk erfassten Daten. Außerdem sind in diesem Abschnitt Informationen zu Netzwerkarchitekturen, Sicherheit und Datenzuordnungen zu finden.

Abschnitt 6 – Störungsanalyse und -beseitigung

Dieser Abschnitt enthält Tipps für die Störungsanalyse und -beseitigung sowie Informationen über die Kontaktaufnahme mit dem technischen Kundendienst per Telefon oder E-Mail.

Abschnitt 7 – Glossar

Dieser Abschnitt enthält Definitionen von Begriffen, die in dieser Betriebsanleitung enthalten sind bzw. die auf dem Web Interface des Smart Wireless Gateway verwendet werden.

Anhänge

Die Anhänge enthalten zusätzliche und spezifischere Informationen über eine Vielzahl von Themen, einschließlich der technischen Daten und Produkt-Zulassungen.

1.4 Service-Unterstützung

Global Service Center
Unterstützung Software und Integration

USA 1 800 833 8314
International +63 2 702 1111

Kundendienst:
Technische Unterstützung, Angebote und Fragen zu Aufträgen

USA 1 800 999 9307 (7 bis 19 Uhr CST)
Asien-Pazifik +65 6777 8211
Europa/Naher Osten/Afrika +49 8153 9390

1.5 Warenrücksendungen

Bezüglich Service Unterstützung sowie Rücklieferung und Reparaturen setzen Sie sich mit Emerson Process Management des jeweiligen Landes (siehe Rückseite dieser Betriebsanleitung) in Verbindung.

In den Vereinigten Staaten wenden Sie sich an das Emerson Process Management Response Center unter der gebührenfreien Telefonnummer 1 800 654 7768. Das Kundendienstzentrum ist rund um die Uhr besetzt, um Ihnen die benötigten Informationen oder Teile bereitzustellen.

Sie müssen die Modell- und Seriennummern des Produktes bereithalten, und es wird Ihnen eine Rücksendegenehmigungs-Nummer für das Produkt (Return Material Authorization [RMA]) zugeteilt. Sie werden auch nach dem Prozessmedium gefragt, dem das Produkt zuletzt ausgesetzt war.

⚠ WARNUNG

Personen, die Produkte handhaben, die gefährlichen Substanzen ausgesetzt sind, können Verletzungen vermeiden, wenn Sie über die Gefahren beim Umgang mit solchen Produkten informiert sind und sich dieser Gefahren bewusst sind. Wenn das zurückgesandte Produkt gefährlichen Substanzen ausgesetzt war, muss bei dessen Rücksendung für jede gefährliche Substanz eine Kopie des Sicherheitsdatenblattes (MSDS) beigefügt werden.

1.6 Produkt-Recycling/Entsorgung

Recycling und Entsorgung des Gerätes und der Verpackung müssen entsprechend den lokalen und nationalen Gesetzgebung/Vorschriften durchgeführt werden.

Abschnitt 2 Erstanschluss

⚠ WARNUNG

Nichtbeachtung dieser Richtlinien zur Installation kann zu schweren oder tödlichen Verletzungen führen:

- Die Installation darf nur von Fachpersonal durchgeführt werden.

Explosionen können zu schweren oder tödlichen Verletzungen führen.

- Sicherstellen, dass die Betriebsatmosphäre des Messumformers den entsprechenden Ex-Zulassungen entspricht.

Elektrische Schläge können schwere oder tödliche Verletzungen verursachen.

- Bei Kontakt mit Leitungen und Anschlüssen äußerst vorsichtig vorgehen.

Dieses Gerät erfüllt Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden Bedingungen: Dieses Gerät darf keine schädliche Störstrahlung verursachen. Dieses Gerät muss Störsignale aufnehmen, auch solche, die zu Betriebsstörungen führen können.

Dieses Gerät ist so zu installieren, dass der Mindestabstand zwischen Antenne und allen Personen 20 cm beträgt.

2.1 Übersicht

Dieser Abschnitt enthält Anweisungen für den erstmaligen Anschluss des Gateway und die zu konfigurierenden Einstellungen, bevor das Gateway mit einem aktiven Leitnetzwerk verbunden wird. Dabei ist zu beachten, dass manche Gateways in eigenständigen Anwendungen verwendet werden und kein Teil eines Netzwerks sind. In diesen Fällen müssen die in diesem Abschnitt aufgeführten Konfigurationseinstellungen jedoch ebenfalls durchgeführt werden.

Bevor das Gateway fest montiert und mit einem aktiven Leitnetzwerk verbunden werden kann, muss eine IP-Adresse für das Gateway konfiguriert werden. Dies erfolgt durch Bildung eines privaten Netzwerks zwischen dem Gateway und einem PC/Laptop. Hierfür sind die folgenden Komponenten erforderlich:

- Gateway
- PC/Laptop
- Verbindungskabel (im Lieferumfang des Gateway enthalten)
- 24-VDC-Spannungsversorgung (nominal)

Hinweis
Wenn das Gateway mit der DeltaV™ Ready Option bestellt wurde, ist es für den Betrieb mit einem DeltaV Leitnetzwerk konfiguriert. In diesem Fall müssen die Anweisungen im Abschnitt „Erstanschluss“ nicht ausgeführt werden, und es ist nur die Einrichtung des Passworts erforderlich.

2.2 Systemanforderungen

Die folgenden Anforderungen gelten für den PC/Laptop, der zum Konfigurieren des Gateway verwendet wird. Bei Verwendung des optionalen Security Setup Utility oder des AMS Wireless Configurator treffen evtl. zusätzliche Anforderungen zu. Weitere Informationen siehe Abschnitt 4: Einrichtung der Software auf Seite 25.

Webbrowser-Programme

- Mozilla® Firefox® 1.5 oder höher
- Microsoft Internet Explorer® 6.0 oder höher

Ethernet

- 10/100base-TX-Ethernet-Kommunikationsprotokoll

2.3 Ersteinstellung

2.3.1 Vorbereitung des PC/Laptop

Der PC/Laptop muss so konfiguriert werden, dass er ein privates Netzwerk bildet, bevor mit dem Gateway kommuniziert werden kann. Die Netzwerkeinstellungen sind in der Systemsteuerung des PC/Laptop zu finden. Konfigurieren der Einstellungen:

1. Die Systemsteuerung öffnen. (Die Systemsteuerung ist gewöhnlich im Startmenü zu finden.)
2. Netzwerkverbindungen öffnen.
3. „LAN-Verbindung“ auswählen.
4. Mit der rechten Maustaste klicken und „Eigenschaften“ aus der Liste auswählen.
5. „Internetprotokoll (TCP/IP)“ auswählen und auf die Schaltfläche „Eigenschaften“ klicken.
6. Auf der Registerkarte *Allgemein* auf die Schaltfläche „Folgende IP-Adresse verwenden“ klicken.
7. Die IP-Adresse auf 192.168.1.12 einstellen und die Tabulatortaste drücken.
8. Die Subnetzmaske 255.255.255.0 sollte automatisch ausgefüllt werden.
9. Auf „OK“ klicken, um das Fenster *Internetprotokoll (TCP/IP)* zu schließen.
10. Im Fenster *LAN-Verbindung* auf die Schaltfläche „Schließen“ klicken.

Internet Proxy-Server müssen über den standardmäßigen Webbrowser des PC/Laptop deaktiviert werden.

1. Den standardmäßigen Internet Browser (gewöhnlich Microsoft Internet Explorer) suchen und öffnen.
2. Das Menü „Extras“ öffnen und „Internetoptionen“ auswählen.
3. Auf der Registerkarte *Verbindungen* auf die Schaltfläche „LAN-Einstellungen“ klicken.
4. Die Kontrollkästchen „Automatische Suche der Einstellungen“ und „Proxyserver für LAN verwenden“ unter *Proxyserver* sollten deaktiviert sein.
5. Auf „OK“ klicken, um das Fenster *LAN-Einstellungen* zu schließen.
6. Auf „OK“ klicken, um das Fenster *Internetoptionen* zu schließen.

Der PC/Laptop ist nun für die Bildung eines privaten Netzwerks und die Kommunikation mit dem Gateway bereit.

Hinweis
Zum Anschluss an den sekundären Ethernet-Port des Gateway müssen die Netzwerkeinstellungen geändert werden. Weitere Netzwerkeinstellungen siehe Tabelle 2-1.

Tabelle 2-1. Standard-IP-Adressen

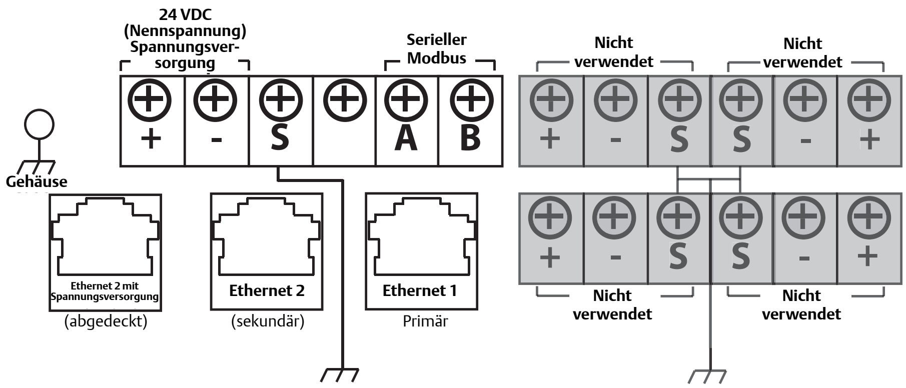
	Gateway	PC/Laptop	Subnet
Ethernet 1	**192.168.1.10**	192.168.1.12	255.255.255.0
Ethernet 2	**192.168.2.10**	192.168.2.12	255.255.255.0
Ethernet 1 (DeltaV Ready)	**10.5.255.254**	10.5.255.200	255.254.0.0
Ethernet 2 (DeltaV Ready)	**10.9.255.254**	10.9.255.200	255.254.0.0

2.3.2 Anschlüsse und Spannungsversorgung

Den PC/Laptop mit dem mitgelieferten Verbindungskabel an das Gateway anschließen. Hierfür ein Ende des Kabels an den Ethernet-Port an der Rückseite des PC/Laptop und das andere Ende an den Ethernet 1 Port des Gateway anschließen. Abbildung 2-1 zeigt das Anschlussschema für den Standard-Anschlussklemmenblock. Nach Herstellung der Verbindung zwischen Gateway und PC/Laptop eine 24-VDC-Spannungsversorgung (nominal) mit mindestens 250-mA-Kapazität an die Spannungseingangsklemmen des Gateway anschließen.

Abbildung 2-1. Standard-Anschlussklemmenblock

.



⚠ WARNUNG

Bei Herstellung der Verbindung zwischen Gateway und PC/Laptop ist es wichtig, die elektrischen Leitungseinführungen an der Unterseite des Gehäuses zu verwenden. Ein Anschluss bei geöffnetem Deckel der Anschlussklemmen-Blockseite (der untere Deckel) kann die Anschlüsse übermäßig belasten und das Gateway beschädigen.

2.3.3 Konfiguration des Gateway

Es ist nun möglich, sich beim Gateway anzumelden und mit der Konfiguration der Einstellungen für den Betrieb in einem aktiven Leitnetzwerk zu beginnen. Die folgenden Einstellungen müssen konfiguriert werden:

- Sicherheitspasswörter
- Zeiteinstellungen
- TCP/IP-Netzwerkeinstellungen

Anmelden beim Gateway:

1. Einen standardmäßigen Webbrowser (gewöhnlich Microsoft Internet Explorer) öffnen.
2. *192.168.1.10* in die Adressleiste eingeben.
3. Die Sicherheitswarnung bestätigen, um fortzufahren.
4. *admin* als Benutzernamen eingeben.
5. *default* als Passwort eingeben.

Der Webbrowser öffnet die standardmäßige Homepage des Gateway. Das Navigationsmenü auf der linken Seite ist in vier Hauptbereiche untergliedert.

- Diagnosefunktionen: Anzeige des Kommunikationsstatus, der Client-Server-Parameter und mehr
- Monitor: Vom Benutzer erstellte Bildschirme zur Anzeige der Daten von Feldgeräten
- Explorer: Basisanzeige von Werten der Feldgeräte
- Einstellung: Konfiguration des Gateway für Betrieb, Sicherheit und Hostsystem-Integration

Sicherheitspasswörter

Das Gateway bietet vier aufgabenbezogene Benutzerkonten mit unterschiedlichen Zugriffsebenen. Die Zugriffsberechtigungen sind in der nachfolgenden Tabelle beschrieben.

Tabelle 2-2. Benutzerkonten der aufgabenbezogenen Zugriffsberechtigungen

Aufgabe	Benutzername	Web-Interface-Zugriff
Leitungspersonal	exec	Nur Lesezugriff
Bediener	oper	Nur Lesezugriff
Wartung	maint	Konfiguration der HART® Geräteeinstellungen Konfiguration der Modbus Kommunikation Konfiguration der Zuordnung von Modbus Registern Konfiguration der OPC Browserstruktur Konfiguration der aktiven Ankündigungen
Administrator	admin	Beinhaltet alle Wartungsprivilegien Konfiguration der Ethernet-Netzwerkeinstellungen Konfiguration der WirelessHART Netzwerkeinstellungen Einstellung der Passwörter Einstellung der Zeiteinstellungen Einstellung der Homepage-Optionen Konfiguration anwenderdefinierter Seiten Neustart von Anwendungen

Die ersten Passwörter der Benutzerkonten wurden auf *default* gesetzt. Aus Sicherheitsgründen wird empfohlen, diese Passwörter zu ändern. Das Administratorpasswort sollte nach dem Ändern sicher aufbewahrt werden. Bei Verlust wenden Sie sich an den technischen Kundendienst von Emerson Process Management.

Ändern der Passwörter der Benutzerkonten:

1. Zu Setup>Security>User Accounts (Einrichtung>Sicherheit>Benutzerkonten) navigieren.
2. Das neue Passwort für jedes aufgabenbezogene Benutzerkonto eingeben und dieses bestätigen.
3. Auf „Submit“ (Übertragen) klicken.

Hinweis
Es wird empfohlen, die standardmäßigen Sicherheitseinstellungen nach der ersten Anmeldung unter Setup>Security>User Options (Einrichtung>Sicherheit>Benutzerkonten) auf die lokalen IT-Vorschriften oder die Einstellung „Normal“ zu ändern. Außerdem stehen die Option „Strong“ bzw. kundenspezifische Einstellungen zur Verfügung, um die Sicherheit der Passwörter zu erhöhen. Weitere Informationen über diesen und andere Bildschirme finden Sie im „User Interface Terminology Guide“ (Terminologie der Benutzeroberfläche) (00809-0605-4420).

Zeiteinstellungen

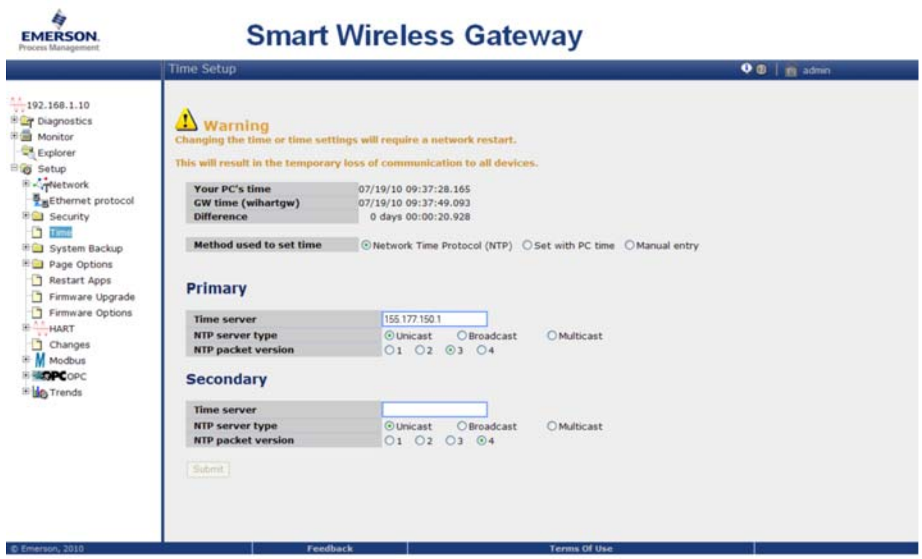
Das Gateway dient als Zeitreferenz für das WirelessHART Netzwerk. Es ist daher wichtig, dass die Zeiteinstellung des Gateway richtig ist, um die Genauigkeit der mit einem Zeitstempel versehenen Daten zu gewährleisten. Die Zeiteinstellungen sind unter Setup>Time (Einrichtung>Zeit) zu finden.

Die Gateway Zeit kann auf drei verschiedenen Arten eingestellt werden:

1. Network Time Protocol (empfohlen).
   Diese Option verwendet einen Network Time Protocol (NTP) Server, um die Zeit des Gateway langsam einzustellen, damit diese mit der Zeit des Leitnetzwerks übereinstimmt. Die IP-Adresse des NTP-Servers eingeben und die Paketversion (1, 2, 3 oder 4) auswählen.
2. Einstellung mittels PC-Zeit.
   Diese Option passt die Zeit des Gateway der Zeit des PC/Laptop an.
3. Manuelle Eingabe.
   Mithilfe dieser Option kann der Benutzer ein bestimmtes Datum (MM:TT:JJ) und eine bestimmte Zeit (HH:MM:SS) eingeben.

Hinweis
Das Network Time Protocol (NTP) passt die Zeit kontinuierlich an die Zeit des Netzwerk-Zeitservers an und wird daher empfohlen, um die optimale Leistung des Netzwerks zu gewährleisten.

Abbildung 2-2. Zeiteinstellungen



TCP/IP-Netzwerkeinstellungen

⚠ WARNUNG

Beim Ändern von TCP/IP-Netzwerkeinstellungen vorsichtig vorgehen. Gehen diese verloren oder sind sie falsch konfiguriert, kann es unmöglich werden, sich beim Gateway anzumelden. Informationen über die richtigen TCP/IP-Netzwerkeinstellungen erhalten Sie vom Netzwerkadministrator.

Vor der Installation und der Verbindung mit einem aktiven Leitnetzwerk müssen die IP-Adresse des Gateway und andere TCP/IP-Netzwerkeinstellungen konfiguriert werden.

Die folgenden Konfigurationspunkte vom Netzwerkadministrator anfordern:

- IP-Adresse spezifizieren oder Verwendung eines DHCP-Servers
- Hostname
- Domainname
- IP-Adresse
- Netzmaske
- Gateway

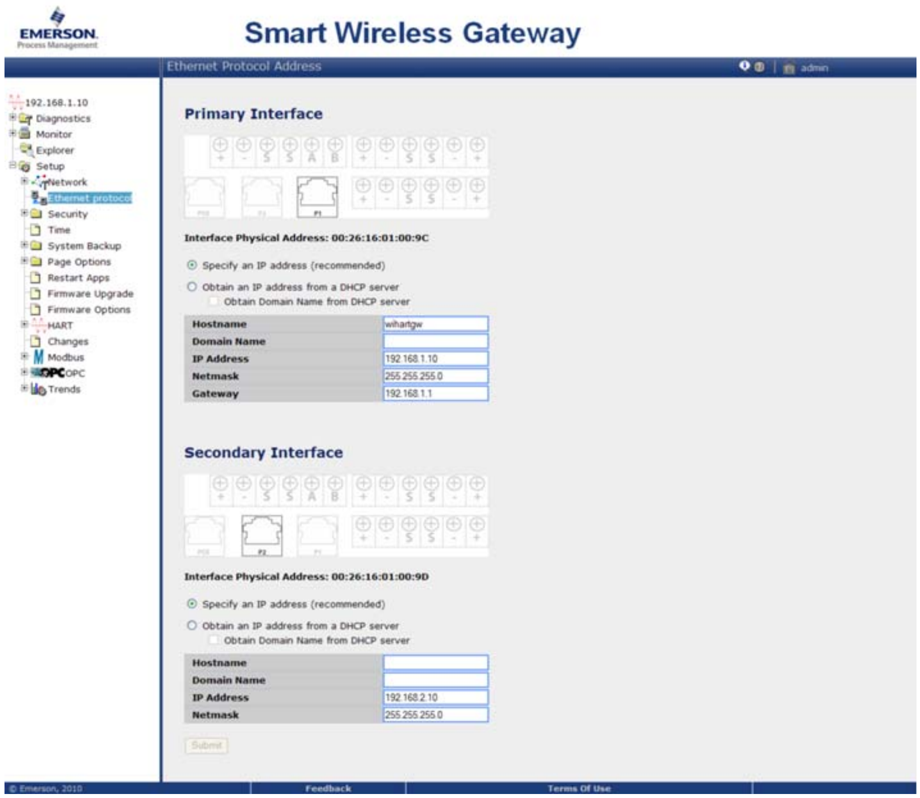
Die Verwendung eines DHCP-Servers zum Erlangen einer IP-Adresse wird nicht empfohlen, da der Betrieb des Gateway in diesem Fall von der Verfügbarkeit des DHCP-Servers abhängig ist. Eine eigene IP-Adresse spezifizieren, um die maximale Verfügbarkeit des Gateway zu gewährleisten.

Ändern der TCP/IP-Netzwerkeinstellungen:

1. Zu Setup>Ethernet Protocol (Einrichtung>Ethernet-Protokoll) navigieren.
2. „Specify an IP address“ (IP-Adresse angeben) (empfohlen) auswählen.
3. Folgendes eingeben:
   - Hostname
   - Domain Name (Domainname)
   - IP Address (IP-Adresse)
   - Netmask (Netzmaske)
   - Gateway
4. Auf „Submit“ (Übertragen) klicken.
5. Nach entsprechender Aufforderung auf „Restart apps“ (Anwendungen neu starten) klicken.
6. Auf „Yes“ (Ja) klicken, um den Neustart zu bestätigen.
7. Den Webbrowser schließen.

Hinweis
Nach dem Ändern der IP-Adresse des Gateway geht die Kommunikation mit dem Web-Interface verloren. Den Webbrowser neu starten und mit der neuen IP-Adresse und anderen TCP/IP-Netzwerkeinstellungen wieder beim Gateway anmelden. Die TCP/IP-Netzwerkeinstellungen des PC/Laptop müssen evtl. auch geändert werden.

Abbildung 2-3. Ethernet-Einstellungen



2.3.4 System Backup

Das Gateway verfügt über ein System Backup und eine Wiederherstellungsfunktion (Restore), die alle benutzerkonfigurierten Daten speichert. Während des Installations- und Konfigurationsverfahrens sollte regelmäßig ein System Backup durchgeführt werden.

1. Zu Setup>System Backup>Save (Einrichtung>System Backup>Speichern) navigieren.
2. Auf „Save Configuration“ (Konfiguration speichern) klicken.
3. Das Gateway sammelt alle Konfigurationsdaten. Wenn das Popup-Fenster für den Datei-Download angezeigt wird, auf „Save“ (Speichern) klicken.
4. Einen Speicherort und Dateinamen eingeben.
5. Auf „Save“ (Speichern) klicken.
6. Auf „Return to form“ (Zurück zum Formular) klicken.

Hinweis
Bei der Datensicherung werden auch die für die Verschlüsselung der Kommunikation verwendeten Benutzerpasswörter gespeichert. Die heruntergeladenen Sicherungsdateien sollten daher an einem sicheren Ort aufbewahrt werden.

Abschnitt 3 Montage und Anschluss

⚠ WARNUNG

Explosionen können zu schweren oder tödlichen Verletzungen führen:

- Sicherstellen, dass die Prozessatmosphäre des Geräts den entsprechenden Ex-Zulassungen entspricht.

Die Elektronik kann durch elektrostatische Entladungen beschädigt werden:

- Vor der Handhabung von Elektronikteilen bzw. vor dem Anschließen von Leitungen und Anschlussklemmen auf die richtige persönliche Erdung achten.

Elektrische Schläge können schwere oder tödliche Verletzungen verursachen. Ist das Gerät in einer Umgebung mit hoher Spannung installiert und eine Störbedingung oder Installationsfehler ereignet sich, kann eine hohe Spannung an den Leitungen und Anschlussklemmen des Geräts anliegen.

- Bei Kontakt mit Leitungen und Anschlüssen äußerst vorsichtig vorgehen.

Nichtbeachtung dieser Richtlinien zur Installation kann zu schweren oder tödlichen Verletzungen führen:

- Die Installation darf nur von Fachpersonal durchgeführt werden.

Dieses Gerät erfüllt Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden Bedingungen: Dieses Gerät darf keine schädlichen Störungen verursachen, alle empfangenen Störungen dürfen keine Auswirkungen zeigen, einschließlich Störungen, die einen unerwünschten Betrieb verursachen.

Dieses Gerät ist so zu installieren, dass der Mindestabstand zwischen Antenne und allen Personen 20 cm beträgt.

3.1 Übersicht

Dieser Abschnitt enthält Anweisungen für die ordnungsgemäße Montage des Gateway und den elektrischen Anschluss, einschließlich der elektrischen Verdrahtung, Erdung und Anschlüsse des Hostsystems. Außerdem sind in diesem Abschnitt Anweisungen zur Montage der optionalen externen Antenne zu finden.

3.1.1 Allgemeine Hinweise

Das Smart Wireless Gateway eignet sich für die Feldmontage im normal üblichen Bereich. Darauf achten, dass die Gehäusedeckel fest verschlossen sind, damit die Elektronik keiner Feuchtigkeit oder Kontamination ausgesetzt wird.

Das Gateway sollte an einem Ort installiert werden, an dem einfacher Zugriff auf das Hostsystem-Netzwerk (Leitnetzwerk) sowie das Wireless-Feldgerätenetzwerk gegeben ist.

3.1.2 Gerätebeschreibung

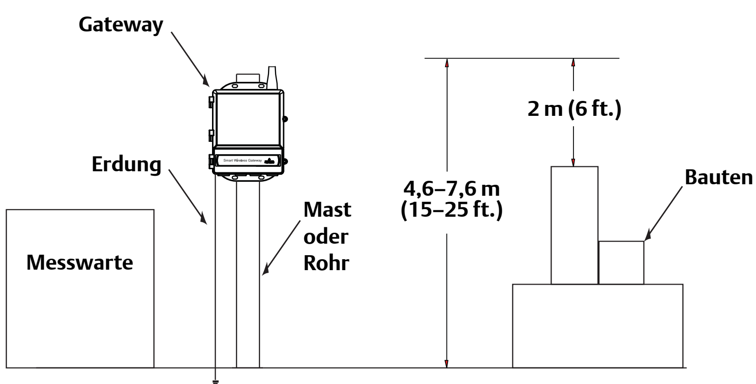
Maßzeichnungen siehe Anhang A: Technische Daten. Die Elektronikplatinen des Gateway sind in einem Gehäuse aus Aluminiumguss untergebracht. An der Vorderseite des Gehäuses ist ein oberer Deckel und der Deckel der Anschlussdose angebracht. Der obere Deckel bietet Zugang zur Elektronik und zum Sender. Der Deckel der Anschlussdose bietet Zugang zum Anschlussklemmenblock.

Zum Öffnen des jeweiligen Deckels die Schraube auf der dem Scharnier gegenüberliegenden Seite des Gehäuses mit einem ¼-Zoll-Schraubendreher entfernen.

3.2 Montage

Das Gateway an einem Ort installieren, an dem optimale Wireless-Leistungsmerkmale gewährleistet sind. Idealerweise 4,6–7,6 m (15–25 ft.) über dem Boden oder 2 m (6 ft.) oberhalb von Hindernissen oder größeren Bauten. Abbildung 3-1 zeigt ein Beispiel für die Installation des Gateway.

Abbildung 3-1. Gateway Installation



3.2.1 Rohrmontage

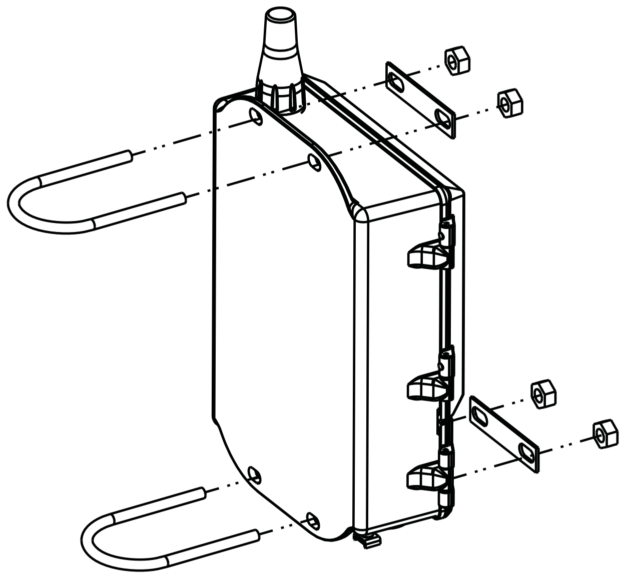
Für die Montage des Gateway an ein 50 mm (2 Zoll) Rohr werden die folgenden Befestigungsteile und Hilfsmittel benötigt:

- Zwei 5/16 Zoll U-Schrauben (mit dem Gateway mitgeliefert)
- 50 mm (2 Zoll) Montagerohr
- ½-Zoll-Schraubenschlüssel

Das Gateway wie folgt montieren:

1. Eine U-Schraube um das Rohr, durch die oberen Montagebohrungen des Gateway Gehäuses und durch die Unterlegplatte einsetzen.
2. Die Muttern auf der U-Schraube mit einem ½-Zoll-Schraubenschlüssel festziehen.
3. Dieses Verfahren mit der zweiten U-Schraube und den unteren Montagebohrungen wiederholen.

Abbildung 3-2. Rohrmontage



3.2.2 Haltermontage (alternativ)

Für die Montage des Gateway an eine Halterung werden die folgenden Befestigungsteile und Hilfsmittel benötigt:

- Vier $^{15}/_{16}$-Zoll-Schrauben
- Montagehalterung
- $^{3}/_{8}$-Zoll-Bohrer
- $^{1}/_{2}$-Zoll-Schraubenschlüssel

Das Gateway wie folgt montieren:

1. Vier 9,525 mm ($^{3}/_{8}$ Zoll) Löcher mit einem horizontalen Abstand von 77 mm (3,06 Zoll) und mit einem vertikalen Abstand von 283 mm (11,15 Zoll) in die Montagehalterungen bohren. Diese Löcher entsprechen den Abständen der Befestigungsbohrungen im Gehäuse des Gateway.
2. Einen $^{1}/_{2}$-Zoll-Schraubenschlüssel verwenden, um das Gateway mit vier $^{15}/_{16}$-Zoll-Schrauben an der Montagehalterung zu befestigen.

3.3 Externe Antenne (optional)

Die Option einer externen Antenne bietet eine flexible Gateway Montage in Bezug auf Wireless-Anschluss, Überspannungsschutz und aktuelle Arbeitsverfahren.

⚠ WARNUNG

Bei der Installation einer extern montierten Antenne für das Smart Wireless Gateway stets die bestehenden Sicherheitsverfahren berücksichtigen, um Beschädigungen oder Kontakt mit Stromleitungen zu vermeiden.

Die Komponenten der externen Antenne für das Smart Wireless Gateway entsprechend den lokalen und nationalen elektrischen Vorschriften sowie den besten Praktiken hinsichtlich Überspannungsschutz installieren.

Vor der Installation mit dem lokalen Abnahmebeauftragten, dem Verantwortlichen und dem Werksabteilungsleiter für elektrische Anlagen in Verbindung setzen.

Die externe Antenne des Smart Wireless Gateway ist speziell dafür ausgelegt, durch Flexibilität bei der Installation die Leistung des Wireless-Netzwerks zu optimieren und lokale Spektrumszulassungen zu erhalten. Um die Leistung des Wireless-Netzwerks zu erhalten und die Nichteinhaltung von Spektrumsvorschriften zu vermeiden, die Länge des Kabels bzw. den Antennentyp nicht ändern.

Wenn der im Lieferumfang enthaltene externe Antennensatz nicht wie in diesem Dokument spezifiziert installiert wird, ist Emerson Process Management nicht für die Wireless-Leistung oder die Nichteinhaltung von Spektrumsvorschriften verantwortlich.

Der externe Antennensatz enthält Koaxialkabel-Abdichtband für den Anschluss der Kabel von Überspannungsschutz und Antenne.

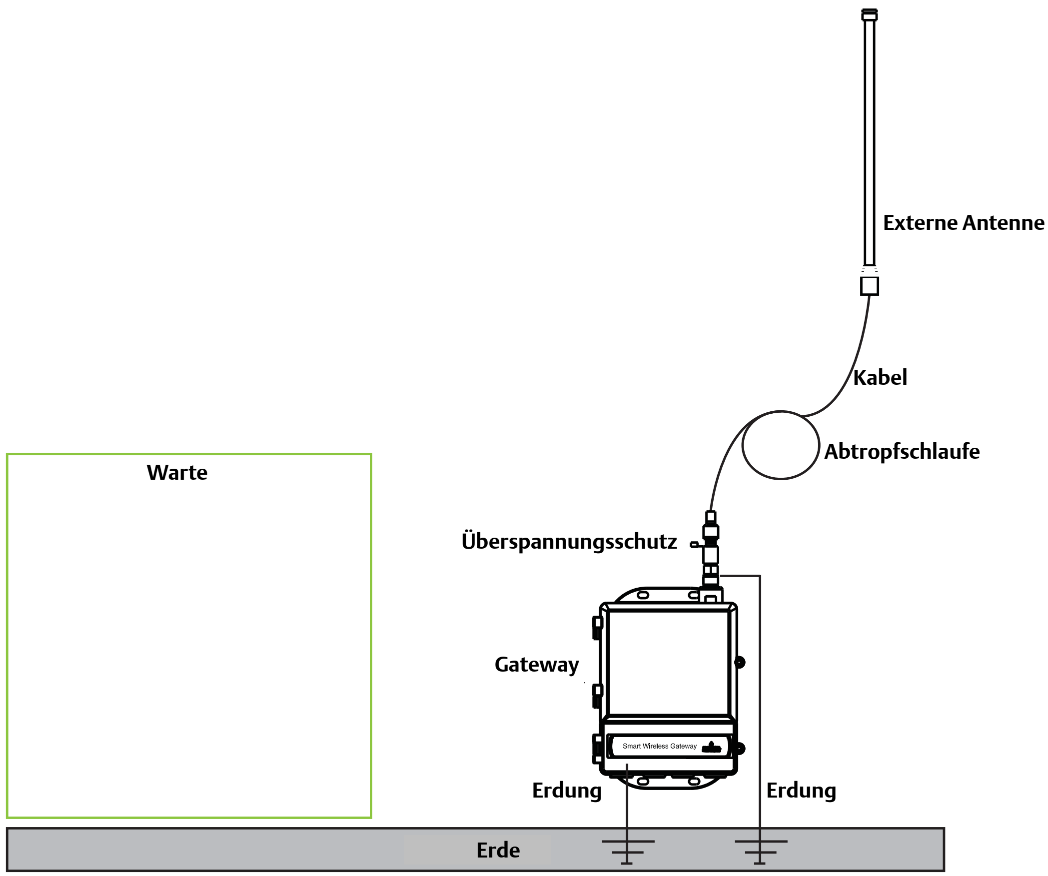
Die externe Antenne an einem Ort installieren, an dem die optimale Wireless-Leistung gewährleistet ist: idealerweise 4,6–7,6 m (15–25 ft.) über dem Boden oder 2 m (6 ft.) oberhalb von Hindernissen oder größeren Bauten. Die externe Antenne mit einem der folgenden Verfahren installieren:

Installation einer WL2/WN2-Option (im Freien):

1. Die Antenne unter Verwendung der im Lieferumfang enthaltenen Befestigungsteile an einen 38–50 mm (1,5–2 Zoll) Rohrmast montieren.
2. Den Überspannungsschutz direkt oben auf das Gateway installieren.
3. Den Erdungsanschluss, die Sicherungsscheibe und die Mutter oben auf dem Überspannungsschutz anbringen.
4. Die Antenne mit dem mitgelieferten Koaxialkabel an den Überspannungsschutz anschließen. Dabei darauf achten, dass die Abtropfschlaufe mindestens 0,3 m (1 ft.) vom Überspannungsschutz entfernt ist.
5. Die einzelnen Anschlüsse von Wireless-Feldgerät, Überspannungsschutz, Kabel und Antenne mit dem Koaxialkabel-Abdichtband abdichten.
6. Sicherstellen, dass Montagerohr, Überspannungsschutz und Gateway entsprechend den lokalen/nationalen elektrischen Vorschriften geerdet sind.

Überschüssiges Koaxialkabel sollte mit einem Durchmesser von 0,3 m (12 Zoll) aufgerollt werden.

Abbildung 3-3. Installation einer WL2/WN2-Option

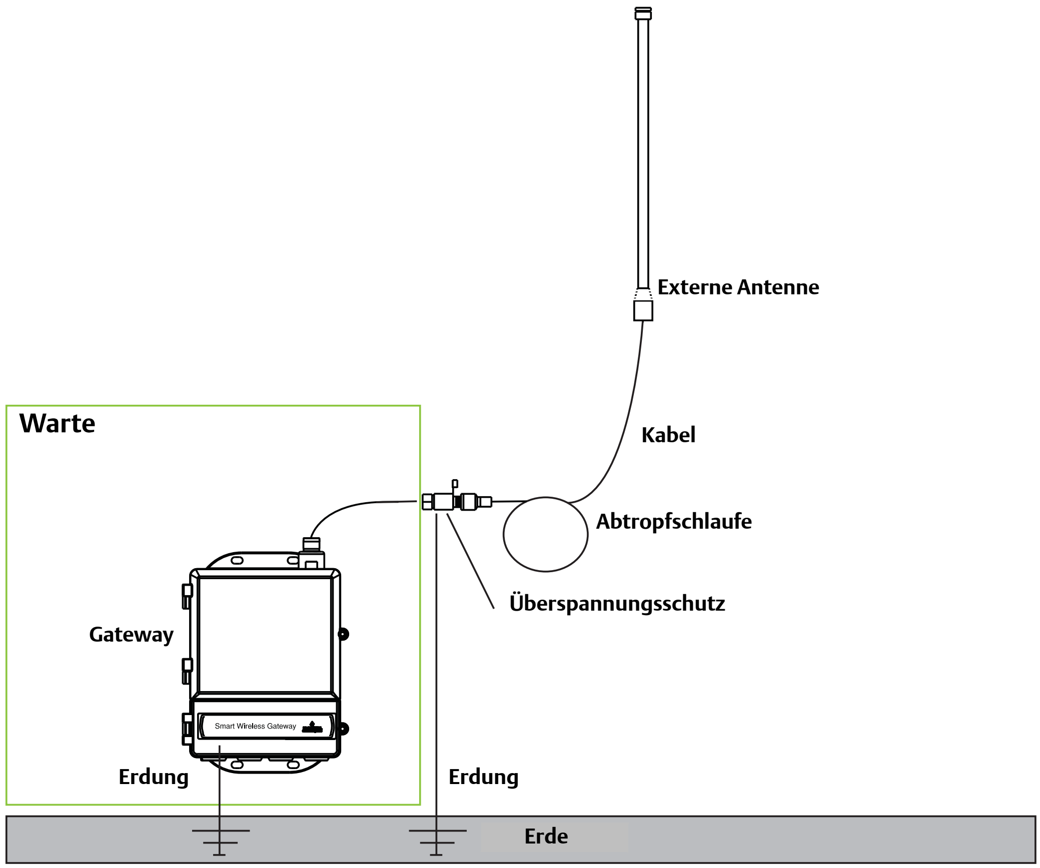


Installation einer WL3/WL4-Option (von Räumen ins Freie):

1. Die Antenne unter Verwendung der im Lieferumfang enthaltenen Befestigungsteile an einen 38–50 mm (1,5–2 Zoll) Rohrmast montieren.
2. Den Überspannungsschutz in der Nähe der Austrittsstelle des Gebäudes montieren.
3. Die Erdungsklemme, Sicherungsscheibe und Mutter oben auf dem Überspannungsschutz anbringen.
4. Die Antenne mit dem mitgelieferten Koaxialkabel an den Überspannungsschutz anschließen. Dabei darauf achten, dass die Abtropfschlaufe mindestens 0,3 m (1 ft.) vom Überspannungsschutz entfernt ist.
5. Den Überspannungsschutz mit dem mitgelieferten Koaxialkabel an das Gateway anschließen.
6. Die einzelnen Anschlüsse von Gateway, Überspannungsschutz, Kabel und Antenne mit dem Koaxialkabel-Abdichtband abdichten.
7. Sicherstellen, dass Montagerohr, Überspannungsschutz und Gateway entsprechend den lokalen/nationalen elektrischen Vorschriften geerdet sind.

Überschüssiges Koaxialkabel sollte mit einem Durchmesser von 0,3 m (12 Zoll) aufgerollt werden.

Abbildung 3-4. Installation einer WL3/WL4-Option



Hinweis: Eine wetterfeste Abdichtung ist erforderlich!
Der externe Antennensatz enthält Koaxialkabel-Abdichtband für den Anschluss der Kabel von Überspannungsschutz, Antenne und Gateway. Das Koaxialkabel-Abdichtband muss verwendet werden, um die Leistung des Wireless-Feldnetzwerks zu gewährleisten. Details für eine wetterfeste Abdichtung sind in Abbildung 3-5 dargestellt.

Abbildung 3-5. Koaxialkabel-Abdichtband an Kabelanschlüsse anbringen

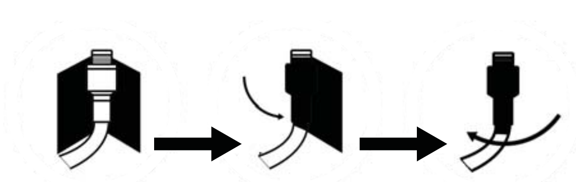


Tabelle 3-1. Optionen externer Antennenkits

Option	Antenne	Kabel 1	Kabel 2	Überspannungsschutz
WL2	$^{1}/_{2}$ Wellenlänge Dipol, Rundstrahlantenne +6 dB Verstärkung	15,2 m (50 ft.) LMR-400	–	Kopfmontage, Buchse/Stecker Gasentladungsrohr 0,5 dB Verlustleistung
WL3	$^{1}/_{2}$ Wellenlänge Dipol, Rundstrahlantenne +6 dB Verstärkung	9,1 m (30 ft.) LMR-400	6,1 m (20 ft.) LMR-400	Inline, Buchse/Buchse Gasentladungsrohr 0,5 dB Verlustleistung
WL4	$^{1}/_{2}$ Wellenlänge Dipol, Rundstrahlantenne +6 dB Verstärkung	12,2 m (40 ft.) LMR-400	3,0 m (10 ft.) LMR-400	Inline, Buchse/Buchse Gasentladungsrohr 0,5 dB Verlustleistung
WN2	$^{1}/_{2}$ Wellenlänge Dipol, Rundstrahlantenne +8 dB Verstärkung	7,6 m (25 ft.) LMR-400	–	Kopfmontage, Buchse/Stecker Gasentladungsrohr 0,5 dB Verlustleistung

3.4 Anschlussverfahren

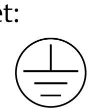
Alle Anschlüsse am Gateway können am Anschlussklemmenblock vorgenommen werden, der in der unteren Anschlussdose des Gehäuses untergebracht ist. Auf der Innenseite des unteren Deckels ist ein Anschlussschema des Anschlussklemmenblocks angebracht. Das Anschlussschema des standardmäßigen Anschlussklemmenblocks ist in Abbildung 3-6 und das Anschlussschema des Glasfaser-Anschlussklemmenblocks in Abbildung 3-8 dargestellt.

Die Anschlussdose des Gehäuses hat vier Leitungseinführungen für die Spannungsversorgungs- und Kommunikationsleitungen. Die Kommunikationsleitungen nicht zusammen mit Spannungsversorgungsleitungen in einem offenen Kabelkanal oder einem Schutzrohr und nicht in der Nähe von Geräten mit hohen elektrischen Spannungen verlegen.

Nicht verwendete Leitungseinführungen mit den im Lieferumfang enthaltenden Verschlussstopfen verschließen. Für Gehäuseschutzarten gemäß NEMA 4X und IP65 Dichtband (PTFE) oder Gewindedichtungsmittel auf das Außengewinde auftragen, um die wasserdichte Abdichtung zu gewährleisten.

3.4.1 Erdung

Das Gehäuse des Gateway muss immer gemäß den örtlichen oder werksinternen Vorschriften für die Elektroinstallation geerdet sein. Die beste Methode zur Erdung ist die direkte Verbindung zur Erde mit minimaler Impedanz. Zur Erdung des Gateway den externen Erdungsanschluss mit Schutzerde verbinden. Die Verbindung sollte einen Widerstand von maximal 1 Ohm aufweisen. Der externe Erdungsanschluss ist unten am Gehäuse des Gateway zu finden und mit dem folgenden Symbol gekennzeichnet:

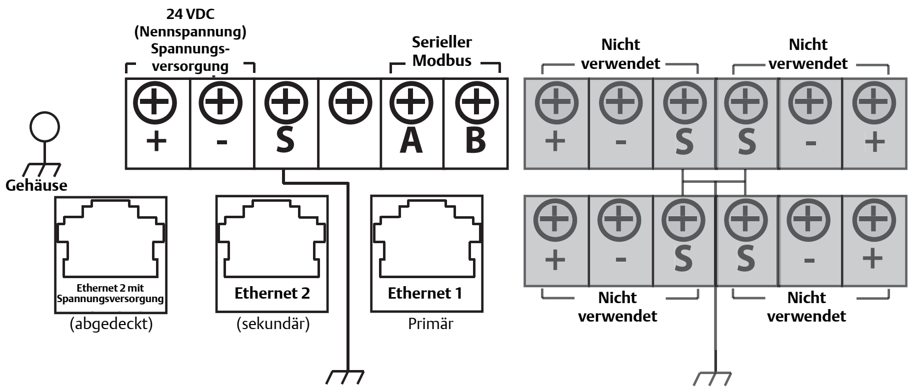


3.4.2 Ethernet

Das Gateway verfügt über zwei 10/100 Based-TX-Ethernet-Kommunikationsanschlüsse (siehe Abbildung 3-6). Diese Anschlüsse ermöglichen den Zugriff auf das Web-Interface des Gateway und die Kommunikation der Modbus TCP und OPC Protokolle.

Der primäre Ethernet Port (Ethernet 1) dient dem Anschluss des Hostsystems oder anderer Anwendungssysteme. Der sekundäre Ethernet Port (Ethernet 2) kann als Reserveanschluss oder als Wartungsanschluss für den lokalen Zugriff auf das Gateway verwendet werden.

Abbildung 3-6. Anschlussschema des Anschlussklemmenblocks



Für die Ethernet-Verbindung mit einem Ethernet-Hub, -Switch oder -Router sollte abgeschirmtes Cat5E-Kabel verwendet werden. Die maximale Kabellänge darf 100 m (328 ft.) nicht überschreiten.

Hinweis
Der sekundäre Ethernet-Port (Ethernet 2) ist nur dann aktiv, wenn bei der Bestellung duale Ethernet-Ports angegeben werden.

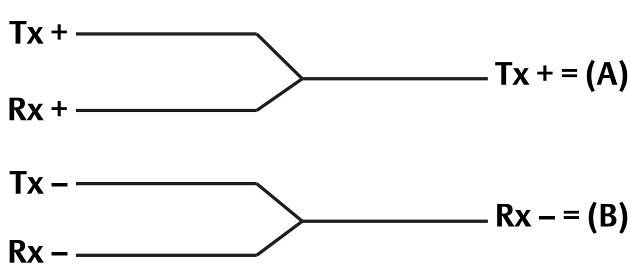
3.4.3 RS-485

Das Gateway kann optional mit einem (seriellen) RS-485 Anschluss bestellt werden (Abbildung 3-6). Die Anschlussklemmen sind in diesem Fall mit A und B Serial Modbus gekennzeichnet. Dieser Anschluss dient der Kommunikation gemäß Modbus RTU auf einem RS-485-Datenbus.

Zum Anschließen des Gateway an den RS-485-Datenbus einzeln abgeschirmte, paarweise verdrillte Adernpaare mit 0,82 mm^2 (AWG 18) Querschnitt verwenden. Die Busgesamtlänge darf 1220 m (4000 ft.) nicht überschreiten. Das Tx + Kabel (Plus, Senden) an die Klemme A und das Rx – Kabel (Minus, Empfangen) an die Klemme B anschließen. Die Kabelabschirmung muss kurz abisoliert und vom Gehäuse des Gateway sowie von anderen Abschlüssen isoliert werden.

Wenn der bestehende Datenbus eine Konfiguration mit 4-Leiter-Vollduplex verwendet, siehe Abbildung 3-7 bzgl. Umrüstung in eine Konfiguration mit 2-Leiter-Halbduplex.

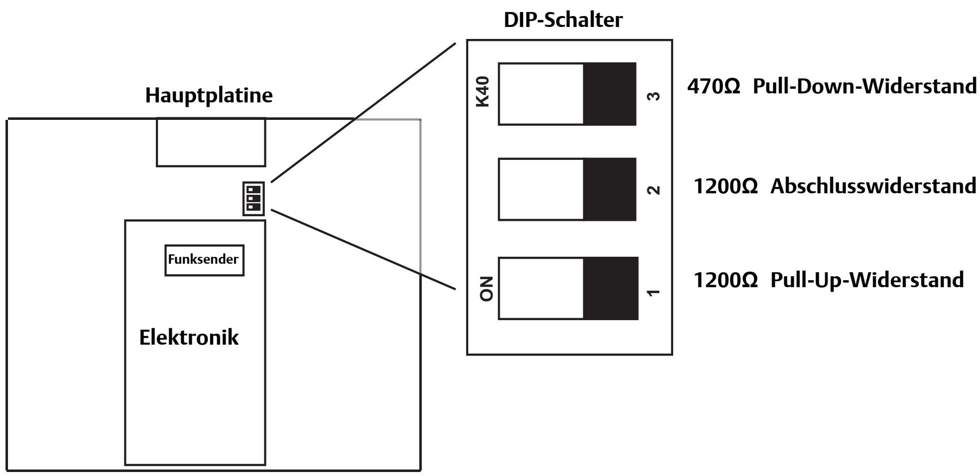
Abbildung 3-7. Umrüstung von Voll- in Halbduplex



3.4.4 Abschlusswiderstände

Mithilfe von drei DIP-Schaltern lassen sich verschiedene Abschlusswiderstände am RS-485-Datenbus aktivieren. Die Schalter sind im Elektronikgehäuse oben in der Mitte auf der Hauptplatine angeordnet (Abbildung 3-8).

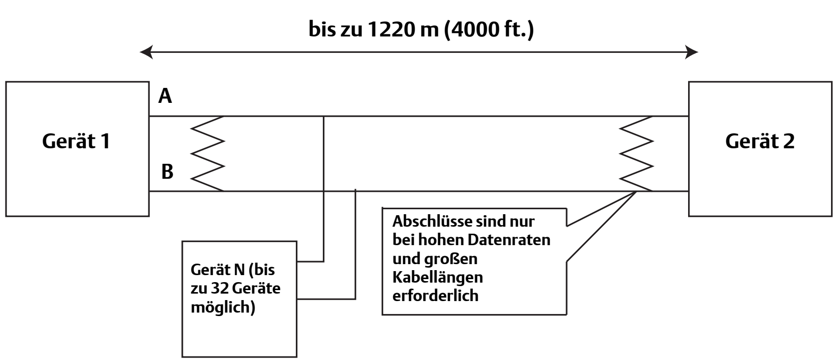
Abbildung 3-8. DIP-Schalter der RS-485-Abschlusswiderstände



Die Schalter 1 und 3 sind mit Pull-up und Pull-down Widerständen verbunden. Schalter 1 steuert die Tx + (A) Leitung und Schalter 3 steuert die Rx – (B) Leitung. Diese 470 Ω-Widerstände verhindern in Perioden, in denen keine Kommunikation stattfindet, dass Signalrauschen als gültige Kommunikation interpretiert wird. Es sollte jeweils nur ein Satz an Pull-up und Pull-down Widerständen auf dem RS-485-Datenbus aktiv sein.

Der Schalter 2 ist mit einem 120 Ω-Abschlusswiderstand verbunden. Dieser Widerstand dient der Dämpfung von Signalreflexionen bei großen Kabellängen. Der Datenbus sollte gemäß RS-485-Spezifikationen an beiden Enden abgeschlossen werden (Abbildung 3-9). Der Abschluss sollte jedoch nur bei hohen Datenraten (über 115 kbps) und großen Kabellängen verwendet werden.

Abbildung 3-9. Typisches (2-Leiter) Halbduplex-Netzwerk



3.4.5 Spannungsversorgung

Das Gateway muss mit 24 VDC (nominal) versorgt werden und erfordert 250 mA Strom. Die Plus- und Minusklemmen sind auf der linken Seite des Anschlussklemmenblocks zu finden (Abbildung 3-6). Ein weiterer Gehäuse-Erdungsanschluss befindet sich auf der linken Seite der Anschlussdose des Gehäuses.

Die Spannungsversorgung an die Plus- (+) und Minusklemme (–) auf der linken Seite des Anschlussklemmenblocks anschließen (Abbildung 3-6). Ein weiterer interner Gehäuse-Erdungsanschluss befindet sich auf der linken Seite des Gehäuses. Die Verdrahtung sollte einen externen Aus- oder Trennschalter in der Nähe des Gateway beinhalten.

Hinweis
Die Verwendung einer unterbrechungsfreien Stromversorgung (USV) wird empfohlen, um die Verfügbarkeit des Gateway bei einem Spannungsausfall zu gewährleisten.

Abschnitt 4 Einrichtung der Software

4.1 Übersicht

Dieser Abschnitt enthält Anweisungen für die Installation und Einrichtung der optionalen Software, die im Lieferumfang des Smart Wireless Gateway enthalten ist. Die Software ist für die Funktion des Wireless-Feldnetzwerks nicht erforderlich, sie erleichtert jedoch die Integration in ein sicheres Hostsystem sowie die Konfiguration von Wireless-Feldgeräten. Die nachfolgende Tabelle enthält eine Beschreibung der einzelnen Anwendungen und zeigt, auf welcher CD diese zu finden sind.

Tabelle 4-1. Softwareanwendungen

Name	Beschreibung	Einbauort
Security Setup Utility (Security Setup Dienstprogramm)	Dieses Dienstprogramm ermöglicht die Einrichtung der SSL-fähigen Kommunikation zwischen Gateway und Hostsystem.	CD 1
AMS Wireless Configurator	Diese Anwendung ermöglicht die vollständige Konfiguration von Wireless-Feldgeräten und bietet zusätzliche Sicherheit durch Bereitstellung mittels Drag&Drop.	CD 2
Network Configuration	Diese Anwendung konfiguriert AMS Wireless Configurator für die Kommunikation mit einem Wireless-Netzwerk oder einem HART Modem.	CD 2

Je nach aktueller Konfiguration des Systems können zusätzliche Systemkomponenten installiert sein.

4.2 Systemanforderungen

Tabelle 4-2. PC-Hardware

Mindestvoraussetzungen	Empfohlene Voraussetzungen
Intel Core 2 Duo, 2,0 GHz	Intel Core 2 Quad, 2,0 GHz oder höher
1 GB Arbeitsspeicher	3 GB Arbeitsspeicher oder größer
1,5 GB freier Festplattenspeicher	2 GB freier Festplattenspeicher oder mehr

Hinweis
SNAP-ON Anwendungen erfordern zusätzlichen Festplattenspeicherplatz. Die Mindestanforderungen an den Monitor sind 1024 x 768 Auflösung und 16-Bit-Farbtiefe.

Tabelle 4-3. Unterstützte Betriebssysteme

Betriebssystem	Ausführung
Windows XP	Professional, Service Pack 3
Windows Server 2003	Standard, Service Pack 2
Windows Server 2003 R2	Standard, Service Pack 2
Windows Server 2008	Standard, Service Pack 2
Windows Server 2008 R2	Standard, Service Pack 1
Windows 7	Professional, Service Pack 1
Windows 7	Enterprise, Service Pack 1

Hinweis
AMS Wireless Configurator unterstützt ausschließlich Betriebssysteme mit 32-Bit-Versionen.

4.3 Installation der Software

Die Software ist auf dem Paket mit 2 CDs zu finden, das im Lieferumfang des Gateway enthalten ist. Die Installation kann je nach Konfiguration des PC-Systems 30–35 Minuten dauern. Es wird empfohlen, zunächst die CD 1 und danach die CD 2 zu installieren. Das Security Setup Dienstprogramm befindet sich auf der CD 1. Software wie folgt installieren:

1. Alle Windows-Programme beenden/schließen, einschließlich aller im Hintergrund laufenden Programme wie Virusscan-Software.
2. Die CD 1 in das CD/DVD-Laufwerk des PCs einlegen.
3. Die Bildschirmanweisungen befolgen.

AMS Wireless Configurator befindet sich auf der CD 2. Die Software wie folgt installieren:

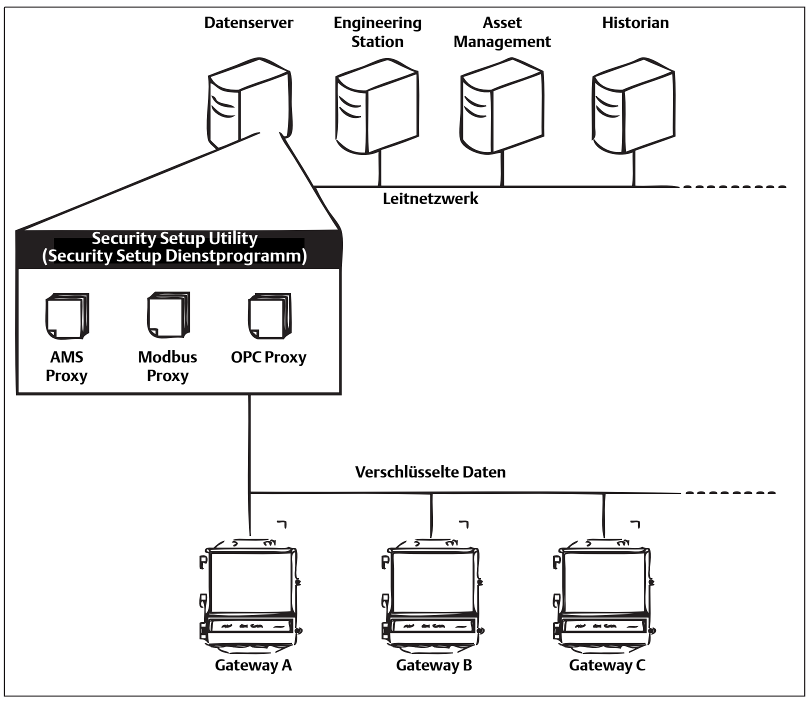
1. Alle Windows Programme beenden/schließen, einschließlich aller im Hintergrund laufenden Programme wie Virusscan-Software.
2. Die CD 2 in das CD/DVD-Laufwerk des PCs einlegen.
3. Wenn das Setup-Programm des AMS Wireless Configurator startet, im Menü auf „Install“ klicken.
4. Die Bildschirmanweisungen befolgen.
5. Dem AMS Wireless Configurator den Neustart des PCs erlauben.
6. Die CD nicht aus dem CD/DVD-Laufwerk herausnehmen.
7. Die Installation läuft nach der Anmeldung automatisch weiter.
8. Die Bildschirmanweisungen befolgen.

Hinweis
Wenn die Autorun-Funktion auf dem PC deaktiviert ist oder die Installation nicht automatisch beginnt, auf die Datei D:\SETUP.EXE (D ist hier das CD/DVD-Laufwerk des PC) doppelklicken und „OK“ wählen.

4.4 Security Setup Dienstprogramm

Das Security Setup Dienstprogramm ermöglicht die sichere Kommunikation zwischen Gateway und Hostsystem, der Asset Management Software, Data Historians und anderen Anwendungen. Hierfür werden die vom Gateway verwendeten standardmäßigen Datenprotokolle (AMS Wireless Configurator, Modbus TCP, EtherNet/IP™ und OPC) verschlüsselt und über verschiedene Proxyserver innerhalb des Security Setup Dienstprogramms verfügbar gemacht. Diese Proxyserver können als Datenserver für andere Anwendungen auf dem Leitnetzwerk fungieren. Das Security Setup Dienstprogramm kann mehrere Gateways gleichzeitig unterstützen, und jeder Proxy unterstützt mehrere Verbindungen mit Client-Anwendungen. Abbildung 4-1 zeigt eine typische Systemarchitektur unter Verwendung des Security Setup Dienstprogramms.

Abbildung 4-1. Typische Hostsystem-Architektur unter Verwendung des Security Setup



Hinweis
Die OPC-Kommunikation erfordert die Verwendung des Security Setup Dienstprogramms unabhängig davon, ob eine Verschlüsselung notwendig ist oder nicht.

4.4.1 Einrichtung

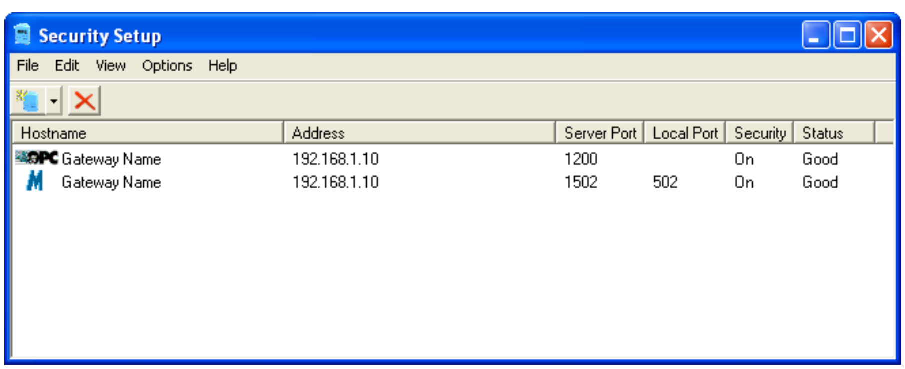
Im Security Setup Dienstprogramm für jedes Gateway einen neuen Proxy basierend auf dem verwendeten Kommunikationsprotokoll hinzufügen. Beispiel: Einen OPC Proxy für jedes Gateway hinzufügen, das OPC als Kommunikationsprotokoll verwendet.

Hinzufügen eines neuen Proxy zum Security Setup Dienstprogramm:

1. Das Security Setup Dienstprogramm öffnen.
2. Auf EDIT>NEW (Bearbeiten>Neu) klicken und dann den Typ des neuen Proxys auswählen, der hinzugefügt werden soll.
3. Mit der rechten Maustaste auf den neuen Proxy-Eintrag klicken und „Properties“ (Eigenschaften) auswählen.
4. Hostname und IP Address (IP Adresse) des Gateway eingeben.
5. Auf „OK“ klicken.
6. Auf FILE>SAVE (Datei>Speichern) klicken.
7. Bei Aufforderung zur Authentifizierung das Administratorkennwort für das Ziel-Gateway eingeben.
8. Auf „OK“ klicken.
9. Die Schritte 2–8 wiederholen, um weitere Proxys hinzuzufügen.
10. Auf FILE >EXIT (Datei>Beenden) klicken, um das Security Setup Dienstprogramm zu schließen.

Bei diesem Verfahren tauscht das Gateway Sicherheitszertifikate (digitale Signaturen) mit dem Proxy aus.

Abbildung 4-2. Security Setup Utility (Security Setup Dienstprogramm)



4.5 AMS Wireless Configurator

Der AMS Wireless Configurator unterstützt die Implementierung und Konfiguration von Wireless-Feldgeräten. Er stellt eine integrierte Betriebsumgebung zur Verfügung, die das gesamte Leistungsspektrum von WirelessHART Geräten (einschließlich integriertem Daten-Trending, grafischer Darstellung und grafischer Anzeigefunktionen, die durch erweiterte EDDL-Technologie bereitgestellt werden) wirksam einsetzt.

- Anzeige und Änderung der Gerätekonfiguration
- Anzeige der Gerätediagnose
- Anzeige von Prozessvariablen
- Bereitstellung eines Wireless-Geräts mittels Drag&Drop, damit es eine Verbindung mit dem selbstorganisierenden Netzwerk eines Gateway herstellen kann
- Verbesserung der Funktionalität des AMS Wireless Configurator mithilfe der AMS Wireless SNAP-ON Anwendung
- Beschränkung des Zugriffs auf Funktionen des AMS Wireless Configurator durch Sicherheitsprivilegien

Die aktuelle Version des AMS Wireless Configurator betreffende Informationen sind in den Versionshinweisen zu finden. Zum Anzeigen der Versionshinweise START>PROGRAMME> AMS WIRELESS CONFIGURATOR>HILFE auswählen.

4.5.1 Einrichtung

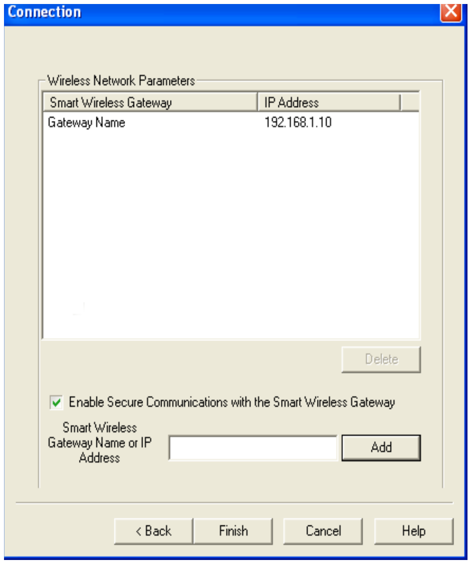
Der AMS Wireless Configurator kann mit einem Wireless-Netzwerk oder einem HART Modem verbunden werden. Beide dieser Schnittstellen müssen über die Network Configuration Anwendung konfiguriert werden. Zum Ausführen dieser Anwendung START>PROGRAMME>AMS DEVICE MANAGER>NETWORK CONFIGURATION auswählen.

Hinweis:
Das Security Setup Dienstprogramm darf nicht gleichzeitig mit der Network Configuration Anwendung ausgeführt werden. Andernfalls kann ein Konfigurationsfehler auftreten.

Konfigurieren eines Wireless-Netzwerks für den AMS Wireless Configurator:

1. Die Anwendung „Network Configuration“ öffnen.
2. Auf Add... (Hinzufügen) klicken.
3. Wireless Network (Wireless-Netzwerk) auswählen und auf Install... (Installieren) klicken.
4. Auf „Next“ (Weiter) klicken.
5. Einen Namen für das Wireless-Netzwerk eingeben und auf Next (Weiter) klicken.
6. HostName (Hostnamen) oder IP Address (IP-Adresse) des Gateway eingeben und auf Add (Hinzufügen) klicken.
7. Schritt 6 wiederholen, wenn mehrere Gateways hinzugefügt werden müssen.
8. Das Kontrollkästchen „Enable Secure Communications with the Smart Wireless Gateway“ (Sichere Kommunikation mit dem Smart Wireless Gateway aktivieren) aktivieren, um diese Funktion zu aktivieren.
9. Auf Finish (Beenden) klicken, um das Konfigurationsfenster zu schließen.
10. Auf Close (Schließen) klicken, um die Anwendung „Network Configuration“ zu beenden.

Abbildung 4-3. Wireless-Netzwerk in der Anwendung „Network Configuration"



Konfigurieren eines HART Modems für den AMS Wireless Configurator:

1. Die Anwendung „Network Configuration" öffnen.
2. Auf Add... (Hinzufügen) klicken.
3. HART modem (HART Modem) auswählen und auf Install... (Installieren) klicken.
4. Auf „Next" (Weiter) klicken.
5. Einen Namen für das HART Modem eingeben und auf Next (Weiter) klicken.
6. Den Typ des HART Master auswählen (die Standardeinstellung in AMS Wireless Configurator ist „Primary HART master") und auf Next (Weiter) klicken.
7. Den COM port (COM-Anschluss) für das HART Modem auswählen und auf Next (Weiter) klicken.
8. Das Kontrollkästchen „Check to support Multi Drop devices" (Aktivieren, um Multidrop-Geräte zu unterstützen) aktivieren, um diese Funktion zu aktivieren.
9. Das Kontrollkästchen „Include WirelessHART Adapter" (WirelessHART Adapter einschließen) aktivieren, um diese Funktion zu aktivieren.
10. Auf Finish (Beenden) klicken, um das Konfigurationsfenster zu schließen.
11. Auf Close (Schließen) klicken, um die Anwendung „Network Configuration" zu beenden.

4.6 Lizenzierung und Quellenangaben

Die neuesten Lizenzvereinbarungen sind auf jeder CD des Softwarepacks enthalten.

„Dieses Produkt umfasst von OpenSSL Project entwickelte Software zur Verwendung im OpenSSL Toolkit. (http://www.openssl.org/)“

„Dieses Produkt umfasst von Eric Young (eay@cryptsoft.com) geschriebene Software.“

Abschnitt 5 Host-Integration

5.1 Übersicht

Dieser Abschnitt enthält Anweisungen für die Verbindung des Gateway mit einem Hostsystem und die Integration der vom Feldgerätenetzwerk erfassten Daten. Außerdem sind in diesem Abschnitt Informationen zu Netzwerkarchitekturen, Sicherheit und Datenzuordnungen zu finden.

5.2 Netzwerkarchitektur

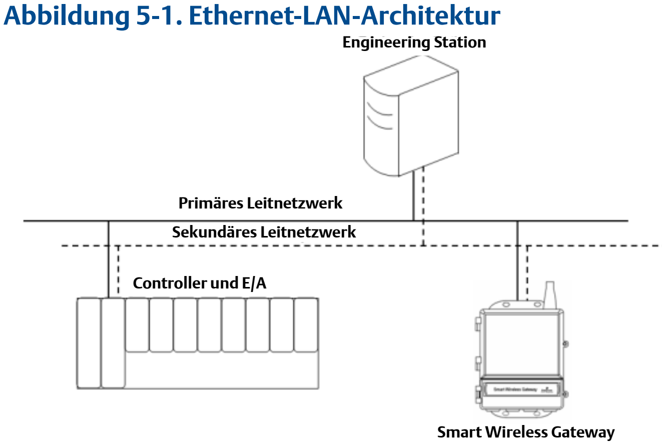
Die Arten der physischen Anschlüsse sind bei der Bestimmung der Netzwerkarchitektur und der für die Integration zu verwendenden Protokolle sehr wichtig. Ethernet ist die primäre physische Anschlussart und RS485 ist als optionale Anschlussart verfügbar. Die folgenden Netzwerkarchitektur-Anschlussschemata sind bei der Integration der Daten vom Gateway in das Hostsystem hilfreich.

In Übereinstimmung mit den Sicherheitsrichtlinien von Emerson WirelessHART sollte das Emerson Gateway über LAN (Local Area Network) und nicht über WAN (Wide Area Network) mit dem Hostsystem verbunden werden.

Ethernet

Eine Ethernet-Verbindung unterstützt die Modbus TCP, OPC, AMS Wireless Configurator, EtherNet/IP und HART TCP-Protokolle. Bei Verwendung dieser Anschlussart wird das Gateway mittels eines Netzwerk-Switches, -Routers oder -Hub direkt mit einem Leitnetzwerk verdrahtet (siehe Abbildung 5-1). Aus Redundanzgründen werden häufig zwei Netzwerke verwendet.

Abbildung 5-1. Ethernet-LAN-Architektur

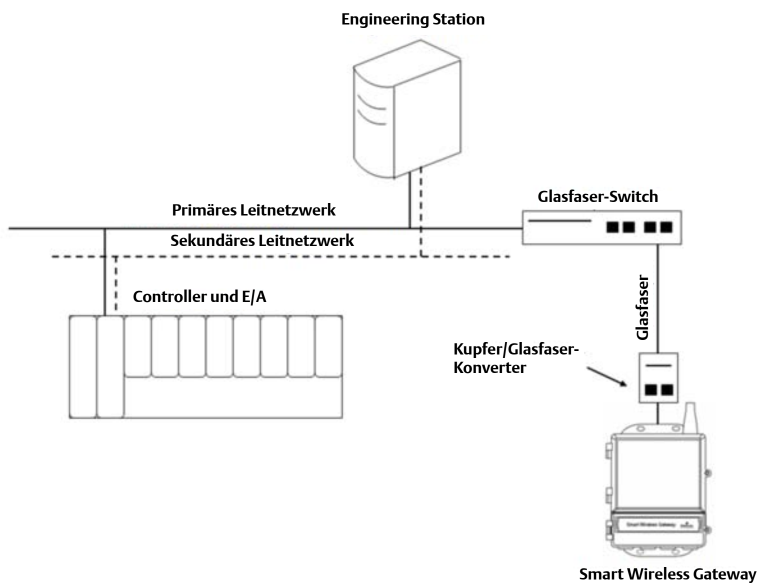


Glasfaser (optional)

Eine Glasfaserverbindung unterstützt die Modbus TCP, OPC, AMS Wireless Configurator und HART TCP Protokolle. Bei Verwendung dieser Anschlussart wird das Gateway mit einem Glasfaser-Switch verdrahtet (siehe Abbildung 5-2).

Hinweis
Eine Glasfaserverbindung erfordert einen Kupfer-Ethernet/Glasfaser-Ethernet-Konverter von einem anderen Hersteller.

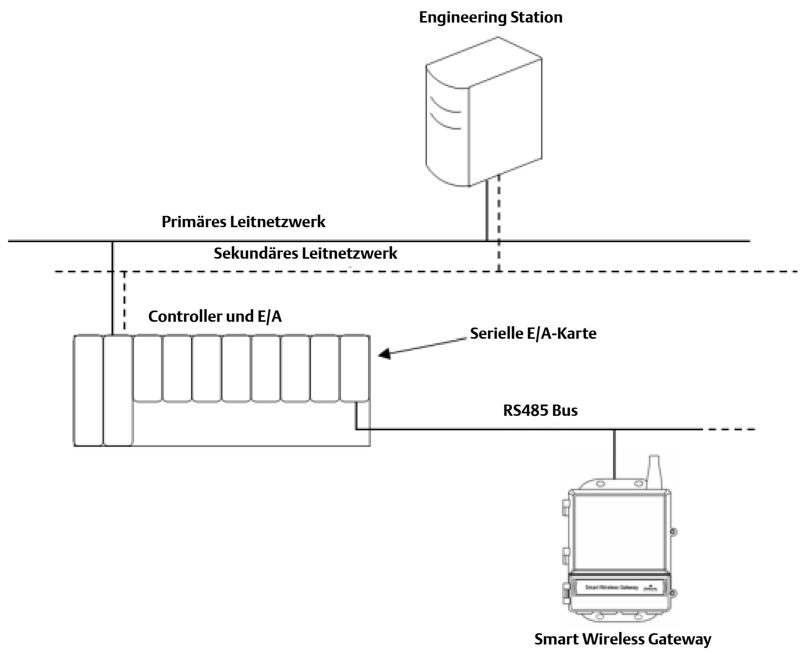
Abbildung 5-2. Glasfaser-LAN-Architektur



RS485 (seriell)

Eine RS485-Verbindung unterstützt das Modbus RTU Protokoll. Bei Verwendung dieser Anschlussart wird das Gateway mit einem RS485 Bus verdrahtet, der gewöhnlich zu einer seriellen E/A-Karte oder einer Modbus E/A-Karte führt (siehe Abbildung 5-3). Auf diese Weise können bis zu 31 Gateways mit einer einzelnen E/A-Karte verbunden werden.

Abbildung 5-3. RS485-LAN-Architektur

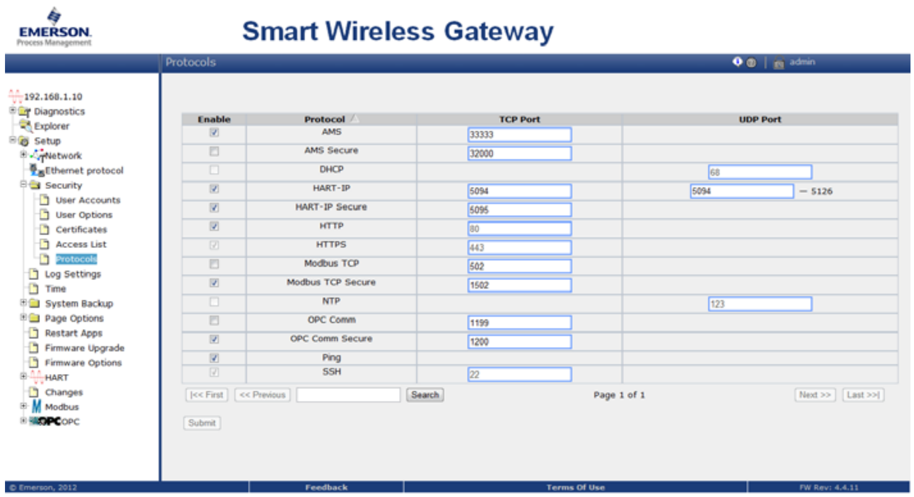


5.3 Interne Firewall

Das Gateway unterstützt eine interne Firewall, die sowohl eingehende als auch ausgehende Datenpakete überprüft. Die TCP-Ports für die Kommunikationsprotokolle sind vom Benutzer konfigurierbar, einschließlich der Portnummern und der Fähigkeit zum Deaktivieren von Ports.

Die Einstellungen der internen Firewall des Gateway sind unter Setup>Security>Protocols (Einrichtung > Sicherheit > Protokolle) zu finden.

Abbildung 5-4. Seite „Sicherheitsprotokolle“ (interne Firewall)



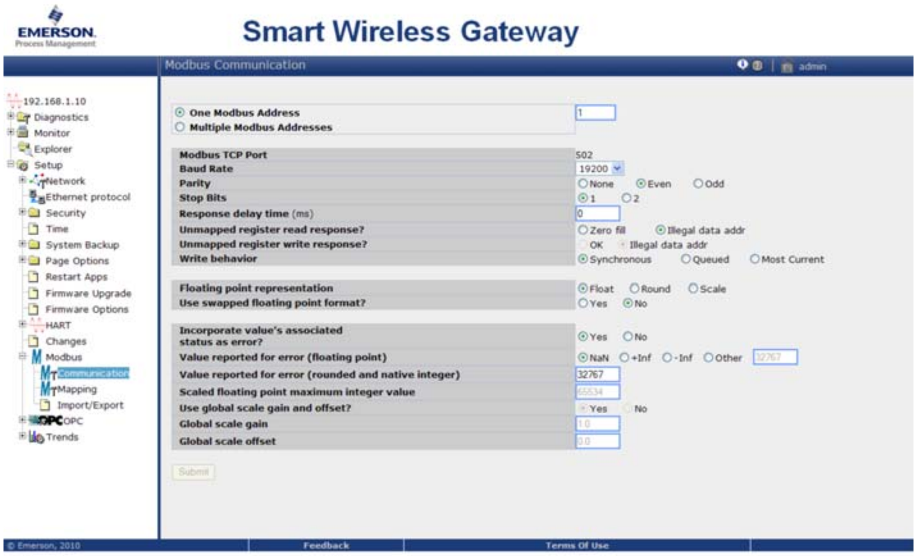
5.4 Modbus

Das Gateway unterstützt sowohl Modbus RTU über den seriellen RS-485-Anschluss als auch Modbus TCP über Ethernet. Es funktioniert als ein Untergerät auf dem Modbus Netzwerk und muss von einem Modbus Master oder Client (Hostsystem) abgefragt werden.

5.4.1 Kommunikationseinstellungen

Es ist zu beachten, dass die Modbus Kommunikationseinstellungen im Gateway mit den Einstellungen im Modbus Master oder Client übereinstimmen müssen. Weitere Informationen über die Konfiguration dieser Einstellungen sind in der Dokumentation des Hostsystems zu finden. Die Modbus-Kommunikationseinstellungen sind unter „Setup>Modbus> Communications“ (Einrichtung>Modbus>Kommunikation) zu finden.

Abbildung 5-5. Seite „Modbus Kommunikation“



One Modbus Address (Einzelne Modbus Adresse): Bei Auswahl dieser Option wird diese Adresse vom Gateway für die Modbus-RTU-Kommunikation verwendet.

Multiple Modbus Addresses (Mehrere Modbus Adressen): Bei Auswahl dieser Option wird eine neue Spalte für Adressen auf der Seite „Modbus Mapping“ (Modbus-Zuordnung) angezeigt.

Modbus TCP-Port: Dies ist der TCP/IP-Port, den das Gateway für Modbus TCP (Ethernet) verwendet. Details zum Ändern der Einstellungen des TCP/IP-Port sind im Abschnitt „Interne Firewall“ zu finden.

Baudrate: Die Datenrate bzw. Übertragungsgeschwindigkeit der seriellen Kommunikation. Diese Einstellung ist nur für Modbus RTU erforderlich.

Parität: Diese Einstellung bestimmt die Parität (keine, gerade oder ungerade), die zur Fehlerprüfung verwendet wird. Diese Einstellung ist nur für Modbus RTU erforderlich.

Stop Bits (Stoppbits): Diese Einstellung bestimmt die Anzahl (1 oder 2) der Stoppbits, die am Ende einer Nachricht verwendet werden soll. Diese Einstellung ist nur für Modbus RTU erforderlich.

Response delay time (ms) (Ansprechzeitverzögerung): Diese Einstellung bestimmt, wie lange das Gateway wartet (in ms), bevor es auf eine Modbus Anforderung reagiert. Diese Einstellung ist nur für Modbus RTU erforderlich.

Unmapped Register Read Response? (Leseantwortzeit, nicht zugeordnete Register?): Dies ist der Wert, der vom Gateway zurückgegeben wird, wenn der Modbus Master ein Register anfordert, dem keine Daten zugeordnet sind (leeres Register). Es wird empfohlen, diesen Wert auf „Zero fill“ (Mit Nullen füllen) zu setzen, um Fehler zu vermeiden.

Floating point representation (Fließkomma-Darstellung): Diese Einstellung bestimmt, ob das Gateway Fließkommawerte oder Ganzzahlwerte verwendet. Es gibt drei Optionen für diese Einstellung:

- Float (Fließkomma): Diese Option verwendet 32-Bit-Fließkommawerte.
- Round (Runden): Diese Option rundet den Datenwert auf die nächste Ganzzahl.
- Scaled (Skaliert): Diese Option verwendet skalierte Ganzzahlen, um negative Werte aufzuheben oder um die Auflösung von Dezimalstellen zu erhöhen. Die Gleichung für skalierte Ganzzahlen lautet:

$$y = Ax – (B – 32768)$$

Wobei:

y = Vom Gateway zurückgegebene skalierte Ganzzahl

A = Verstärkung des skalierten Ganzzahlwerts

x = Vom Wireless-Feldgerät gemessener Wert

B = Offset des skalierten Ganzzahlwerts

Use swapped floating point format? (Getauschtes Fließkommaformat verwenden?): Mit dieser Einstellung kann getauscht werden, welches Register zuerst für einen Fließkommawert gesendet wird. Diese Einstellung wird nur für Fließkommawerte verwendet.

Incorporate value’s associated status as error? (Den Werten zugeordneten Status als Fehler einbeziehen?): Diese Einstellung führt dazu, dass das Gateway einen festgelegten Wert meldet, wenn vom Wireless-Feldgerät ein Kommunikations- oder kritischer Diagnosefehler empfangen wird. Der Wert kann vom Benutzer abhängig von der gewählten Fließkomma-Darstellung konfiguriert werden. Siehe „Value reported for error“ (Als Fehler gemeldeter Wert).

Value reported for error (floating point) (Als Fehler gemeldeter Wert [Fließkomma]): Diese Einstellung bestimmt, welcher Wert ausgegeben wird, wenn das Wireless-Feldgerät einen Ausfall meldet oder nicht mit dem Gateway kommuniziert. Diese Einstellung wird für Fließkommawerte verwendet. Auswahlmöglichkeiten sind NaN (keine Zahl), +Inf (positiv unendlich), –Inf (negativ unendlich) oder Other (benutzerdefiniert).

Value reported for error (rounded and native integer) (Als Fehler gemeldeter Wert [gerundete und native Ganzzahl]): Diese Einstellung bestimmt, welcher Wert ausgegeben wird, wenn das Wireless-Feldgerät einen Ausfall meldet oder nicht mit dem Gateway kommuniziert. Die Einstellung wird für gerundete oder skalierte Ganzzahlen verwendet. Es kann ein benutzerdefinierter Wert zwischen -32768 und 65535 spezifiziert werden.

Scaled floating point maximum integer value (Maximale Ganzzahl eines skalierten Fließkommawerts): Diese Einstellung bestimmt den maximalen Ganzzahlwert zum Zweck der Skalierung von Ganzzahlen. 999-65534.

Use global scale gain and offset? (Globale[n] Skalierungsverstärkung und -offset verwenden?): Diese Einstellung bestimmt, ob eine globale Verstärkung und ein globaler Offset auf skalierte Ganzzahlen angewandt werden sollen oder ob jeder Wert eine spezifische Verstärkung und einen spezifischen Offset aufweist. Spezifische Verstärkungen und spezifische Offsets sind auf der Seite „Modbus Mapping“ (Modbus Zuordnung) zu finden.

Global scale gain (Globale Skalierungsverstärkung): Dieser Wert wird mit den Datenwerten multipliziert, um Ganzzahlen zu skalieren. Wenn keine globale Skalierung ausgewählt wird, steht für jeden separaten Datenwert ein Verstärkungswert auf der Seite „Modbus Mapping“ zur Verfügung.

Global scale offset (Globaler Skalierungsoffset): Dieser Wert wird zu den Datenwerten addiert, um Ganzzahlen zu skalieren. Wenn keine globale Skalierung ausgewählt wird, steht für jeden separaten Datenwert ein Offsetwert auf der Seite „Modbus Mapping“ zur Verfügung.

5.4.2 Registerzuordnung

Bei der Registerzuordnung werden den Modbus Registern Datenpunkte von Wireless-Feldgeräten zugeordnet. Diese Register können dann von einem Modbus Master oder Client gelesen werden. Die Zuordnung von Modbus Registern ist unter Setup>Modbus> Mapping (Einrichtung>Modbus>Zuordnung) zu finden.

Abbildung 5-6. Seite „Modbus Registerzuordnung“



Hinzufügen einen neuen Datenpunkts zur Modbus Registerzuordnung:

1. Auf „New entry“ (Neuer Eintrag) klicken.
2. Alle Tabellenwerte für den neuen Datenpunkt ausfüllen (die Eingabespalten können je nach Modbus Kommunikationseinstellungen variieren).
3. Die Eingabe für jeden neuen Datenpunkt wiederholen.
4. Auf „Submit“ (Übertragen) klicken.
5. Nachdem alle Änderungen akzeptiert wurden, auf „Return to form“ (Zurück zum Formular) klicken.

Adresse: Dies ist die Modbus RTU-Adresse, die vom Gateway für diesen Datenpunkt verwendet wird. Datenpunkte können durch Zuordnen der gleichen Adresse gruppiert werden (d. h. alle Datenpunkte von der gleichen Prozessausrüstung können die gleiche Adresse haben). Diese Spalte wird nur bei Auswahl von „Multiple Modbus Addresses“ (Mehrere Modbus Adressen) auf der Seite „Modbus Communications“ (Modbus Kommunikation) angezeigt.

Register: Dies ist die Nummer des Modbus Registers, das für diesen Datenwert verwendet wird. Modbus Register können Informationen mit zwei Byte (16 Bit) Länge aufnehmen; 32-Bit-Fließkomma- und Ganzzahlen erfordern daher zwei Modbus Register. Jeder Datenpunkt benötigt eine eindeutige Modbus Registernummer, außer wenn Datenpunkte unterschiedlichen Adressen zugeordnet werden. Die Registernummern 0–19999 sind für boolesche Werte (Bit, Speicher, binär usw.) reserviert. Die Registernummern ab 20000+ sind für Fließkomma- und Ganzzahlwerte reserviert.

Point Name (Name des Punktes): Dies ist ein zweiteiliger Name für den Datenpunkt. Der erste Teil ist die HART Messstellenkennzeichnung des Wireless-Feldgeräts, das die Daten liefert. Der zweite Teil ist der Parameter des Wireless-Feldgeräts.

Der Name des Datenpunktes wird als *<HART Messstellenkennzeichnung.PARAMETER>* eingegeben. Die Eingabe kann mithilfe der Werteliste (...) oder manuell erfolgen. Die folgende Tabelle zeigt eine Liste von standardmäßigen Geräteparametern, die Modbus Registern zugeordnet werden können.

Tabelle 5-1. Verfügbare Geräteparameter

Parameter	Beschreibung	Datentyp
PV	Primärvariable	32-Bit-Fließkomma
SV	Sekundärvariable	32-Bit-Fließkomma
TV	Tertiärvariable	32-Bit-Fließkomma
QV	Quartärvariable	32-Bit-Fließkomma
RELIABILITY	Ein Maß für die Konnektivität mit dem Gateway	32-Bit-Fließkomma
ONLINE	Status der Wireless-Kommunikation	Boolean
PV_HEALTHY	Zustandsstatus der PV	Boolean
SV_HEALTHY	Zustandsstatus der SV	Boolean
TV_HEALTHY	Zustandsstatus der TV	Boolean
QV_HEALTHY	Zustandsstatus der QV	Boolean

PV, SV, TV und QV (dynamische Variablen) sind vom Gerätetyp abhängig. Weitere Informationen über den Wert, den jede dynamische Variable repräsentiert, sind in der Gerätedokumentation zu finden.

RELIABILITY und ONLINE beziehen sich auf die Wireless-Kommunikation. RELIABILITY ist der Prozentsatz der vom Wireless-Feldgerät empfangenen Nachrichten. ONLINE ist eine Wahr/Falsch-Angabe, ob das Gerät auf dem Wireless-Netzwerk kommuniziert.

_HEALTHY Parameter sind Wahr/Falsch-Angaben des Zustand einer bestimmten Variable (= dynamische Variable – PV, SV usw.). Diese Parameter liefern kritische Diagnoseinformationen vom Wireless-Feldgerät sowie den Kommunikationsstatus.

Hinweis
Die **_HEALTHY Parameter bieten eine effektive Anzeige des Zustands und des Kommunikationsstatus der Datenwerte.

State (state value) (Zustand) (Zustandswert): Der Wert eines Datenpunkts, der zu einem Modbus Ausgang von 1 führt. Wenn ein Datenpunkt beispielsweise als Wahr oder Falsch gemeldet wird, liefert der Zustandswert „Wahr" eine „1" für Wahr und eine „0" für Falsch. Ein Zustand von „Falsch" liefert eine „0" für Wahr und eine „1" für Falsch. Der Zustand ist nur für Registernummern 0–19999 (Boolesche Werte, Bit, Speicher, binär usw.) erforderlich.

Invert (Invertieren): Bei Markierung dieses Kontrollkästchens wird der Modbus Ausgang von 1 auf 0 oder von 0 auf 1 invertiert. Die Invertierung wird nur für boolesche Werte mit Registernummern 0–19999 verwendet.

Gain (Verstärkung): Dieser Wert wird mit den Datenwerten multipliziert, um Ganzzahlen zu skalieren. Die Verstärkung ist dann erforderlich, wenn „Scaled" (Skaliert) auf der Seite „Modbus Communications" ausgewählt wurde und globale Verstärkung sowie globaler Offset nicht ausgewählt wurden.

Offset: Dieser Wert wird zum Datenwert addiert, um Ganzzahlen zu skalieren. Der Offset ist nur dann erforderlich, wenn „Scaled" (Skaliert) auf der Seite „Modbus Communications" ausgewählt wurde und globale Verstärkung sowie globaler Offset nicht ausgewählt wurden.

Vordefinierte Modbus Register

Zusätzlich zu den benutzerkonfigurierbaren Parametern unterstützt das Gateway außerdem eine Reihe vordefinierter Modbus Register mit Diagnose und Testparametern. Die folgende Tabelle enthält eine Liste der vordefinierten Modbus Register.

Tabelle 5-2. Vordefinierte Modbus Register

Beschreibung	Register	Datentyp
Aktuelles Jahr (1)	49001	32-Bit-Ganzzahl
Aktueller Monat (1)	49002	32-Bit-Ganzzahl
Aktueller Tag (1)	49003	32-Bit-Ganzzahl
Aktuelle Stunde (1)	49004	32-Bit-Ganzzahl
Aktuelle Minute (1)	49005	32-Bit-Ganzzahl
Aktuelle Sekunde (1)	49006	32-Bit-Ganzzahl
Empfangene Nachrichten	49007	32-Bit-Ganzzahl
Fehlerhaft empfangene Nachrichten	49008	32-Bit-Ganzzahl
Mit Ausnahme gesendete Nachrichten	49009	32-Bit-Ganzzahl
Anzahl gesendeter Nachrichten	49010	32-Bit-Ganzzahl
Ignorierte gültige Nachrichten	49011	32-Bit-Ganzzahl
Konstante Fließkommazahl 12345,0	49012	32-Bit-Fließkomma
SYSTEM_DIAG.HART_DEVICES	49014	32-Bit-Ganzzahl
SYSTEM_DIAG.ADDITIONAL_STATUS_0	49015	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_1	49016	8-Bit-Ganzzahl ohne Vorzeichen

Beschreibung	Register	Datentyp
SYSTEM_DIAG.ADDITIONAL_STATUS_2	49017	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_3	49018	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_4	49019	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_5	49020	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_6	49021	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_7	49022	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_8	49023	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_9	49024	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_10	49025	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_11	49026	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.ADDITIONAL_STATUS_12	49027	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.UNREACHABLE	49028	32-Bit-Ganzzahl
SYSTEM_DIAG.UPTIME	49029	32-Bit-Ganzzahl
SYSTEM_DIAG.TEST_BOOLEAN	49031	Boolean
SYSTEM_DIAG.TEST_BYTE	49032	8-Bit-Ganzzahl
SYSTEM_DIAG.TEST_UNSIGNED_BYTE	49033	8-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.TEST_SHORT	49034	16-Bit-Ganzzahl
SYSTEM_DIAG.TEST_UNSIGNED_SHORT	49035	16-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.TEST_INT	49036	32-Bit-Ganzzahl
SYSTEM_DIAG.TEST_UNSIGNED_INT	49038	32-Bit-Ganzzahl ohne Vorzeichen
SYSTEM_DIAG.TEST_FLOAT	49040	32-Bit-Fließkomma

5.5 EtherNet/IP

Kommunikationseinstellungen

Es ist zu beachten, dass die EtherNet/IP-Kommunikationseinstellungen im Gateway mit den Einstellungen im EtherNet/IP Master oder Client übereinstimmen müssen. Weitere Informationen über die Konfiguration dieser Einstellungen sind in der Dokumentation des Hostsystems oder in der Betriebsanleitung für EtherNet/IP (Dok.-Nr. 00809-0505-4420) zu finden. Die EtherNet/IP-Kommunikationseinstellungen sind unter „Setup>EtherNet/IP> Communications" (Einrichtung>EtherNet/IP>Kommunikation) zu finden. Die Netzwerkarchitekturen sollten der eines DeltaV Systems entsprechen (siehe Abbildung C-1 auf Seite 68).

Hinweis
EtherNet/IP kann mit einem beliebigen EtherNet/IP-ODVA-Mitglied integriert werden. Andere Protokolle wie HART-IP funktionieren weiterhin im Gateway. Die vollständigen Bestellinformationen sind im Produktdatenblatt (Dok.-Nr. 00813-0205-4420) zu finden.

Abbildung 5-7. Seite „EtherNet/IP-Kommunikation"

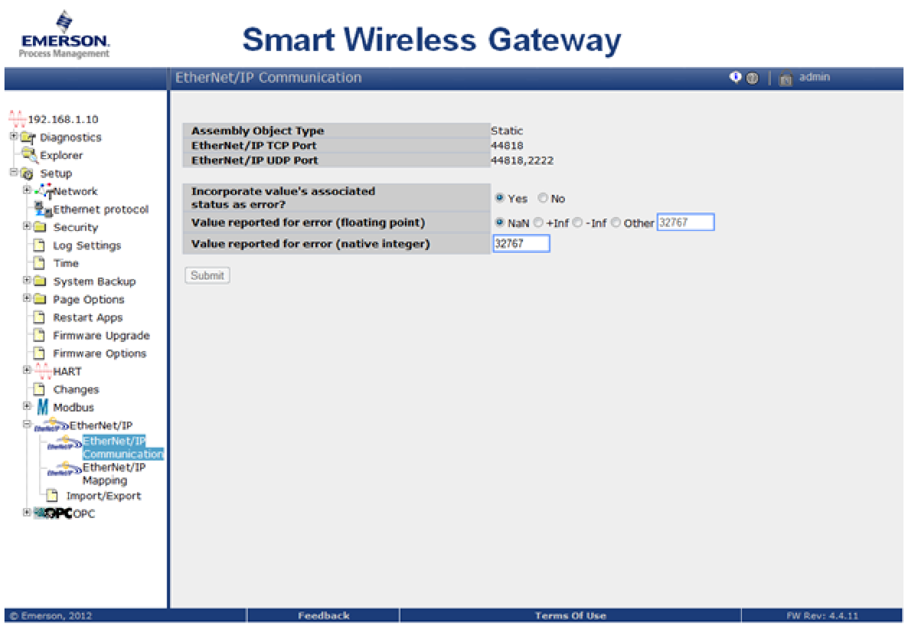


Tabelle 5-3. Setup>EtherNet/IP>EtherNet/IP Communication (Einrichtung>EtherNet/IP>EtherNet/IP Kommunikation)

Begriff	Beschreibung
Assembly Object Type	Von EtherNet/IP verwendetes statisches Assembly-Objekt.
EtherNet/IP TCP Port	Der für den direkten Zugriff auf EtherNet/IP-TCP-Daten vom Gateway verwendete TCP-Port.
EtherNet/IP UDP Ports	Die für den direkten Zugriff auf EtherNet/IP-UDP-Daten vom Gateway verwendeten UDP-Ports.
Incorporate value's associated status as error? (Den Werten zugeordneten Status als Fehler einbeziehen?)	Wenn der Status der HART Variablen eine kritische Störung angibt oder wenn die Kommunikation verloren geht, wird dies durch das EtherNet/IP-Mitglied gemeldet.
Value reported for error (floating point) (Als Fehler gemeldeter Wert [Fließkomma])	Ermöglicht die Auswahl des Werts, der ausgegeben wird, wenn der dem Wert zugeordnete Status eine kritische Störung angibt. Wird nur verwendet, wenn das Gateway für Fließkomma-Darstellung konfiguriert wurde.
NaN	Es wird „keine Zahl" ausgegeben, wenn der dem Wert zugeordnete Status eine kritische Störung angibt.
+Inf	Es wird „positiv unendlich" ausgegeben, wenn der dem Wert zugeordnete Status eine kritische Störung angibt.
–Inf	Es wird „negativ unendlich" ausgegeben, wenn der dem Wert zugeordnete Status eine kritische Störung angibt.
Other	Es wird ein anwenderdefinierter Wert ausgegeben, wenn der dem Wert zugeordnete Status eine kritische Störung angibt.
Value reported for error (native integer) (Als Fehler gemeldeter Wert [native Ganzzahl])	Es wird ein anwenderdefinierter Wert ausgegeben, wenn der dem Wert zugeordnete Status eine kritische Störung angibt. Wird nur verwendet, wenn das Gateway für Ganzzahl-Darstellung konfiguriert wurde.

Unmapped parameter read response? (Leseantwortzeit, nicht zugeordnete Parameter?): Dies ist der Wert, der vom Gateway zurückgegeben wird, wenn der EtherNet/IP Master ein Register anfordert, dem keine Daten zugeordnet sind (leeres Register). Es wird empfohlen, diesen Wert auf „Zero fill" (Mit Nullen füllen) zu setzen, um Fehler zu vermeiden.

Parameter-Zuordnung

Bei der Registerzuordnung werden den EtherNet/IP-Registern Datenpunkte von Wireless-Feldgeräten zugeordnet. Diese Register können dann von einem EtherNet/IP Master oder Client gelesen werden. Die Zuordnung von EtherNet/IP-Registern ist unter Setup>EtherNet/IP>Mapping (Einrichtung>EtherNet/IP>Zuordnung) zu finden.

Abbildung 5-8. Seite „EtherNet/IP Register Map“



Tabelle 5-4. Übersicht über die Begriffe auf der Seite „EtherNet/IP Mapping“ (EtherNet/IP-Zuordnung)

Begriff	Beschreibung
Input Instance	Statische Assembly-Instanz des EtherNet/IP-Eingangs – 496 Byte.
Output Instance	Statische Assembly-Instanz des EtherNet/IP-Ausgangs – 496 Byte.
Member	EtherNet/IP Instanz-Mitglied, in dem Daten erzeugt oder verarbeitet werden.
Point Name	Im Format HARTtag.parameter zugeordneter Datenpunkt.
New entry	Erstellt einen neuen Eintrag in dieser Tabelle.
<<First	Navigiert zur ersten Seite dieser Tabelle.
<<Previous	Navigiert zur vorherigen Seite dieser Tabelle.
Search	Sucht das nächste Auftreten der in dieses Feld eingegebenen Zeichen.
Next>>	Navigiert zur nächsten Seite dieser Tabelle.
Last>>	Navigiert zur letzten Seite dieser Tabelle.
Delete Selected	Entfernt den ausgewählten Eintrag aus dieser Tabelle.
Select All	Wählt alle Einträge der Tabelle aus.
Select None	Hebt die Auswahl aller Einträge der Tabelle auf.
Select Errors	Wählt alle Einträge der Tabelle aus, die eine Fehlermeldung aufweisen.
Submit	Akzeptiert alle Änderungen (gelb markiert).

Hinzufügen eines neuen Datenpunkts zur EtherNet/IP-Registerzuordnung:

1. Auf New entry (Neuer Eintrag) klicken.
2. Alle Tabellenwerte für den neuen Datenpunkt ausfüllen (die Eingabespalten können je nach EtherNet/IP-Kommunikationseinstellungen variieren).
3. Die Eingabe für jeden neuen Datenpunkt wiederholen.
4. Auf „Submit“ (Übertragen) klicken.
5. Nachdem alle Änderungen akzeptiert wurden, auf „Return to form“ (Zurück zum Formular) klicken.

Die Optionen der Parameter, die zugeordnet werden können, sind in Tabelle 5-1 auf Seite 40 aufgeführt.

Abschnitt 6 Störungsanalyse und -beseitigung

Hinweis
Weitere Informationen sind im „User Interface Terminology Guide“ (Terminologie der Benutzeroberfläche) (Dok.-Nr. 00809-0605-4420) zu finden.

Dieser Abschnitt enthält Tipps zur grundlegenden Störungsanalyse und -beseitigung für das Smart Wireless Feldnetzwerk. So erhalten Sie technische Unterstützung per Telefon:

Unterstützung Software und Integration vom Global Service Center.

- USA – 1 800 833 8314
- International – +63 2 702 1111

Technische Unterstützung, Angebote und Fragen zu Aufträgen

- USA – 1 800 999 9307 (7.00 Uhr bis 19 Uhr CST)
- Asien-Pazifik – +65 6777 8211
- Europa/Naher Osten/Afrika – +49 (0) 8153 9390

Oder wenden Sie sich per E-Mail an einen Wireless-Spezialisten:

Specialists-Wireless.EPM-RTC@EmersonProcess.com

Erstanschluss	
Rückgabeseite des Webbrowsers nicht gefunden	1. Gateway und PC/Laptop mit dem mitgelieferten Verbindungskabel verbinden. 2. Überprüfen, ob das Gateway mit 24 VDC (nominal) und 250 mA versorgt wird. Den oberen Deckel öffnen und überprüfen, ob Anzeigeleuchten aufleuchten. 3. Überprüfen, welcher Ethernet-Port am Gateway verwendet wird. 4. Die IP-Adresse des Gateway überprüfen (der standardmäßige primäre Port ist 192.168.1.10, der standardmäßige sekundäre Port ist 192.168.2.10; beim DeltaV Ready Gateway ist der standardmäßige primäre Port 10.5.255.254 und der standardmäßige sekundäre Port 10.9.255.254). 5. Überprüfen, ob die IP-Adresse des PC/Laptop im Subnetz-Bereich des Gateway liegt (d. h. wenn die Gateway IP-Adresse 155.177.0.xxx ist, dann sollte die IP-Adresse des PC/Laptop 155.177.0.yyy sein). 6. Die Proxy-Einstellungen des Internet Browsers deaktivieren.
Gateway wird nach dem Ändern der IP-Adresse nicht gefunden	1. Überprüfen, ob die IP-Adresse des PC/Laptop im Subnetz-Bereich des Gateway liegt (d. h. wenn die Gateway IP-Adresse 155.177.0.xxx ist, dann sollte die IP-Adresse des PC/Laptop 155.177.0.yyy sein).
Gateway wird bei Verwendung des sekundären Ethernet-Ports nicht gefunden	1. Überprüfen, welcher Ethernet-Port am Gateway verwendet wird. 2. Die IP-Adresse des Gateway überprüfen (der standardmäßige primäre Port ist 192.168.1.10, der standardmäßige sekundäre Port ist 192.168.2.10). 3. Überprüfen, ob die IP-Adresse des PC/Laptop im Subnetz-Bereich des Gateway liegt (d. h. wenn die Gateway IP-Adresse 155.177.0.xxx ist, dann sollte die IP-Adresse des PC/Laptop 155.177.0.yyy sein).
Keine Anmeldung beim Gateway möglich	1. Den Benutzernamen und das Passwort überprüfen. Der Benutzername des Administrators ist „admin“ und das standardmäßige Passwort ist „default“. Siehe Tabelle 2-1.

AMS Wireless Configurator	
Gateway wird nicht im AMS Wireless Configurator angezeigt	1. Überprüfen, ob das Security Setup Dienstprogramm auf dem gleichen PC wie AMS Wireless Configurator installiert ist. 2. Mithilfe der Network Configuration Anwendung eine Schnittstelle für die Kommunikation mit einem Wireless-Netzwerk einrichten. Siehe Abschnitt 4: Einrichtung der Software. 3. Überprüfen, ob die Schnittstelle für das Wireless-Netzwerk für Secure Gateway Communications konfiguriert ist. 4. Die Einstellungen für das sichere/nicht gesicherte AMS Wireless Configurator Protokoll auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > SECURITY > PROTOCOLS (Einrichtung > Sicherheit > Protokolle) navigieren. 5. Den AMS Wireless Configurator Datenserver neu starten. Mit der rechten Maustaste auf das Symbol des AMS Wireless Configurator Servers im Windows Infobereich (unten rechts) klicken und „Stop Server“ (Server stoppen) auswählen.
Wireless-Geräte werden nicht unter dem Gateway angezeigt	1. Überprüfen, ob Wireless-Geräte mit dem Gateway verbunden sind. Beim Gateway anmelden und zu EXPLORER navigieren. 2. Mit der rechten Maustaste auf „Wireless Network“ (Wireless-Netzwerk) klicken und „Rebuild Hierarchy“ (Hierarchie neu aufbauen) auswählen.
Wireless-Geräte werden mit rotem HART Symbol angezeigt	1. Die neuesten Supportdateien der Geräte vom AMS Wireless Configurator installieren. Gehen Sie zu www.emersonprocess.com > BRANDS > AMS SUITE > AMS DEVICE MANAGER > DEVICE DESCRIPTION (DDs).
Elemente der Gerätekonfiguration sind grau gemacht	1. Überprüfen, ob aktuelle oder historische Informationen angezeigt werden. Diese Einstellung wird am unteren Rand jedes Gerätekonfigurations-Bildschirms angezeigt. Die Konfiguration erfordert die Einstellung „Current“ (Aktuell). 2. Aus Sicherheitsgründen werden Sitzungen, die mehr als 30 Minuten inaktiv waren, durch einen Konfigurations-Timeout abgemeldet. Beim AMS Wireless Configurator erneut anmelden.

Wireless-Feldgeräte	
Wireless-Geräte werden nicht auf dem Netzwerk angezeigt	1. Die ordnungsgemäße Spannungsversorgung des Geräts überprüfen. 2. Überprüfen, ob sich das Gerät innerhalb der Kommunikationsreichweite befindet. 3. Überprüfen, ob die ordnungsgemäße Network ID (Netzwerkkennung) in das Gerät eingegeben wurde.
Wireless-Gerät wird in der Liste Verbindungsfehler (Join Failure) angezeigt	1. Die Netzwerkkennung und den Verbindungsschlüssel erneut in das Gerät eingeben.
Wireless-Gerät wird mit der Meldung „Service denied“ angezeigt	1. Die Gesamtanzahl der Geräte im Netzwerk (max. 100) überprüfen. 2. Unter SETUP > NETWORK > BANDWIDTH (Einrichtung > Netzwerk > Bandbreite) auf „Analyze Bandwidth“ (Bandbreite analysieren) klicken. (Hinweis: Jegliche Änderungen erfordern eine Neubildung des Netzwerks.) 3. Die Aktualisierungsrate für das Gerät verringern.

Modbus Kommunikation	
Keine Kommunikation über Modbus RTU	1. Überprüfen, ob der RS-485-Anschluss verwendet wird. 2. Die Verdrahtungsanschlüsse überprüfen. Siehe Abschnitt 3: Montage und Anschluss. 3. Überprüfen, ob ein Abschluss erforderlich ist. 4. Überprüfen, ob die Einstellungen für die serielle Modbus Kommunikation auf dem Gateway mit den Einstellungen auf dem Modbus Hostsystem übereinstimmen. Beim Gateway anmelden und zu SETUP > MODBUS > COMMUNICATIONS (Einrichtung > Modbus > Kommunikation) navigieren. 5. Die Modbus Adresse des Gateway überprüfen. 6. Die Zuordnung der Modbus Register auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > MODBUS > MAPPING (Einrichtung > Modbus > Zuordnung) navigieren.
Keine Kommunikation über Modbus TCP	1. Die Einstellungen für das sichere/nicht gesicherte Modbus Protokoll auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > SECURITY > PROTOCOLS (Einrichtung > Sicherheit > Protokolle) navigieren. 2. Die Einstellungen für die Modbus TCP Kommunikation auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > MODBUS > COMMUNICATIONS (Einrichtung > Modbus > Kommunikation) navigieren. 3. Die Zuordnung der Modbus Register auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > MODBUS > MAPPING (Einrichtung > Modbus > Zuordnung) navigieren.
Keine Kommunikation über sicheres Modbus TCP	1. Überprüfen, ob das Security Setup Dienstprogramm installiert wurde. 2. Einen sicheren Modbus Proxy für das Gateway konfigurieren. Siehe Abschnitt 4: Einrichtung der Software. 3. Die Einstellungen für das sichere/nicht gesicherte Modbus Protokoll auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > SECURITY > PROTOCOLS (Einrichtung > Sicherheit > Protokolle) navigieren. 4. Die Einstellungen für die Modbus TCP Kommunikation auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > MODBUS > COMMUNICATIONS (Einrichtung > Modbus > Kommunikation) navigieren. 5. Die Zuordnung der Modbus Register auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > MODBUS > MAPPING (Einrichtung > Modbus > Zuordnung) navigieren.

OPC Kommunikation	
OPC Anwendung findet keinen Gateway OPC Server	1. Überprüfen, ob das Security Setup Dienstprogramm auf dem gleichen PC wie die OPC Anwendung installiert ist. 2. Einen OPC Proxy für das Gateway konfigurieren. Siehe Abschnitt 4: Einrichtung der Software.
Gateway OPC Server zeigt keine Gateways an	1. Einen OPC Proxy für das Gateway konfigurieren. Siehe Abschnitt 4: Einrichtung der Software.
Gateway OPC Server zeigt keine Datenmarkierungen an	1. Die Gateway OPC Browser Struktur konfigurieren. Beim Gateway anmelden und zu SETUP > OPC > OPC BROWSE TREE (Einrichtung > OPC > OPC Browser Struktur) navigieren. 2. Den Verbindungsstatus des OPC Proxy im Security Setup Dienstprogramm überprüfen. 3. Überprüfen, ob der OPC Proxy für sichere oder nicht gesicherte Kommunikation konfiguriert ist. 4. Die Einstellungen für das sichere/nicht gesicherte OPC Protokoll auf dem Gateway überprüfen. Beim Gateway anmelden und zu SETUP > SECURITY > PROTOCOLS (Einrichtung > Sicherheit > Protokolle) navigieren. 5. Die Einstellungen von Netzwerk-Firewall und -Ports überprüfen.

EtherNet/IP	
Gateway gibt keine Parameter aus	Sicherstellen, dass die Verbindung mit EtherNet/IP hergestellt wurde. Zu SETUP > SECURITY > PROTOCOLS (Einrichtung > Sicherheit > Protokolle) navigieren. Siehe Dok.-Nr. 00809-0505-4420: Installationsanleitung bzgl. der Verbindungsaufnahme mit einem Allen Bradley System.

Abschnitt 7 Glossar

Dieser Abschnitt enthält Definitionen von Begriffen, die in dieser Betriebsanleitung enthalten sind bzw. die auf dem Web-Interface des Smart Wireless Gateway verwendet werden.

Begriff	Definition
Access Control List (Zugangskontrollliste)	Eine Liste aller Geräte, die zum Verbinden mit dem Netzwerk zugelassen wurden. Jedes Gerät verfügt außerdem über einen eindeutigen Verbindungsschlüssel. Diese Liste wird auch als „weiße Liste“ bezeichnet.
Active Advertising (Aktive Ankündigung)	Ein Betriebszustand der Netzwerkverwaltung, der dazu führt, dass das gesamte Wireless-Feldnetzwerk Nachrichten sendet, um nach neuen oder nicht erreichbaren Geräten zu suchen und diese mit dem Netzwerk zu verbinden.
Baud Rate (Baudrate)	Die Übertragungsgeschwindigkeit des Modbus RTU.
Burst Rate (Burstrate)	Das Intervall, in dem Wireless-Feldgeräte Mess- und Statusdaten an das Gateway übertragen. Entspricht der Aktualisierungsrate.
Certificate (Zulassung)	Eine digitale Signatur zur Authentifizierung eines Client/Servers bei verschlüsselter Kommunikation.
Connectivity (Konnektivität)	Beschreibt gewöhnlich eine Kombination der Kommunikationsstatistiken und Verbindungszuverlässigkeit eines Wireless-Feldgeräts. Kann außerdem die Verbindung zwischen Gateway und Hostsystem beschreiben.
Device ID (Gerätekennung)	Eine Hexadezimalzahl, die eine eindeutige Identifikation des Geräts ermöglicht.
DHCP	Dynamisches Host-Konfigurationsprotokoll: Verwendet zur automatischen Konfiguration der TCP/IP-Parameter eines Geräts.
Domain (Domäne)	Ein eindeutiger Bezeichner im Internet, beinhaltet durch Punkte getrennte Symbole, wie: this.domain.com
Gateway	Siehe Smart Wireless Gateway.
HART Tag (HART Messstellenkennzeichnung)	Die elektronische Kennzeichnung des Geräts, die vom Gateway für alle Host-Integrationszuordnungen verwendet wird. Bezeichnet die lange HART Messstellenkennzeichnung (32 Zeichen, für HART 6 oder 7 Geräte) oder die HART Meldung (32 Zeichen, nur für verkabelte HART 5 Geräte, die mittels WirelessHART Adapter verbunden werden).
Host Name (Hostname)	Ein eindeutiger Bezeichner in einer Domäne, der mit der IP-Adresse eines Geräts assoziiert ist, wie: device.this.domain.com. In diesem Beispiel ist „device“ (Gerät) der Hostname.
HTML	Hyper Text Markup Language: Das Dateiformat, das zum Erstellen der mit einem Webbrowser angezeigten Seiten verwendet wird.
HTTP	Hyper Text Transfer Protocol: Das Protokoll, das definiert, wie ein Webserver Daten zu einem Webbrowser sendet und von einem Webbrowser empfängt.
HTTPS	HTTP über einen verschlüsselten Secure Sockets Layer (SSL)
Join Failure (Verbindungsfehler)	Wenn ein Wireless-Feldgerät keine Verbindung mit dem WirelessHART Netzwerk herstellen kann. Die meisten Verbindungsfehler werden aus Sicherheitsgründen verursacht (fehlender oder falscher Verbindungsschlüssel, nicht auf der Zugangskontrollliste aufgeführt usw.).
Join Key (Verbindungsschlüssel)	Ein hexadezimaler Sicherheitscode, der es Wireless-Feldgeräten ermöglicht, eine Verbindung mit dem Wireless-Feldnetzwerk herzustellen. Dieser Code muss auf dem Gerät und auf dem Gateway identisch sein.

Begriff	Definition
Latency (Wartezeit)	Der Zeitraum zwischen dem Absenden einer Nachricht vom Wireless-Feldgerät bis zum Empfang durch das Gateway.
Netmask (Netzmaske)	Eine aus 1 und 0 bestehende Zeichenkette, die den Netzwerkteil einer IP-Adresse ausblendet und nur die Hostkomponente anzeigt.
Network I.D. (Netzwerkkennung)	Ein Zifferncode, der Wireless-Feldgeräte dem Gateway zuordnet. Dieser Code muss auf dem Gerät und auf dem Gateway identisch sein.
Network Manager (Netzwerk-Manager)	Eine Betriebsfunktion des Smart Wireless Gateway, die alle Geräteverbindungen und den zeitlichen Ablauf der Wireless-Daten automatisch verwaltet.
NTP	Network Time Protocol. Ein Protokoll, das die Systemzeit mit dem Zeitserver eines Netzwerks synchronisiert.
Path (Übertragungsweg)	Eine Wireless-Verbindung zwischen zwei Geräten in einem Wireless-Netzwerk. Diese Verbindung wird außerdem als „Hop“ bezeichnet.
Path Stability (Weg-Stabilität)	Ein Maß für die Konnektivität zwischen zwei Geräten im Wireless-Netzwerk. Dieser Wert wird als Verhältnis der Anzahl empfangener Nachrichten zur Anzahl erwarteter Nachrichten berechnet.
Primary Interface (Primäre Schnittstelle)	Ethernet 1- oder Glasfaser-Port, der für die primäre Hostkommunikation verwendet wird.
Private Network/LAN (Privates Netzwerk/LAN)	Eine lokale Verbindung zwischen einem Smart Wireless Gateway und einem PC/Laptop. Dieses Netzwerk wird für die Inbetriebnahme und Konfiguration des Gateway verwendet.
Reliability (Zuverlässigkeit)	Ein Maß für die Konnektivität zwischen dem Gateway und einem Wireless-Feldgerät. Dieser Wert wird als Verhältnis der Anzahl empfangener Nachrichten zur Anzahl erwarteter Nachrichten berechnet. Hierbei werden alle Übertragungswege berücksichtigt.
RSSI	Anzeige der Stärke des Empfangssignals (dBm) für das Wireless-Feldgerät.
Secondary Interface (Sekundäre Schnittstelle)	Ethernet 2 Port, der als Backup-Anschluss oder als Serviceanschluss für den lokalen Zugriff verwendet wird.
Security Setup Utility (Security Setup Dienstprogramm)	Eine Softwareanwendung, die die sichere Kommunikation zwischen Gateway und Hostsystem, der Asset Management Software, Data Historians und anderen Anwendungen ermöglicht.
Self-Organizing Network (Selbstorganisierendes Netzwerk)	Mesh-Netzwerk-Technologie, bei der alle Geräteverbindungen und der zeitliche Ablauf der Wireless-Daten automatisch durch eine Netzwerkverwaltung gesteuert werden.
Service Denied (Service abgelehnt)	Das Gerät hat keine Bandbreitenkapazität erhalten und kann keine regelmäßigen Aktualisierungen veröffentlichen.
TCP/IP	Transmission Control Protocol/Internet Protocol. Das Protokoll, das angibt, wie Daten über das Ethernet übertragen werden.
Update Rate (Aktualisierungsrate)	Das Intervall, in dem Wireless-Feldgeräte Mess- und Statusdaten an das Gateway übertragen. Entspricht der Burstrate.
Wireless Field Device(s) (Wireless-Feldgerät[e])	WirelessHART Feldgeräte, die Teil eines Wireless-Feldnetzwerks sind.
Wireless Field Network (Wireless-Feldnetzwerk)	WirelessHART Netzwerk, das aus dem Smart Wireless Gateway und mehreren Wireless-Feldgeräten besteht.
Wireless Plant Network (Wireless-Anlagennetzwerk)	Industrielles WiFi-Netzwerk, das zur Integration des Wireless-Feldnetzwerks in das Leitnetzwerk verwendet wird.

Anhang A Technische Daten

A.1 Funktionsdaten

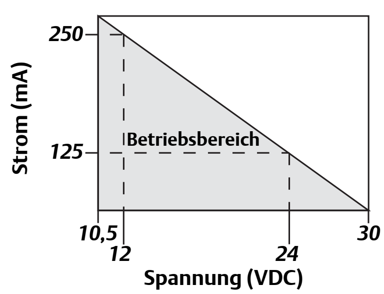
Eingangsspannung

10,5–30 VDC

Stromaufnahme

Stromaufnahme im Betrieb ausgehend von 3,6 Watt Leistungsaufnahme.

Kurzzeitige Stromaufnahme beim Start bis zum Doppelten der Stromaufnahme im Betrieb.



Sendefrequenz-Leistungsausgang von der Antenne

Max. 10 dBm (10 mW) EIRP

Max. 16 dBm (40 mW) EIRP für hohe Antennenverstärkung (Option WN2)

Umgebungsbedingungen

Betriebstemperaturbereich:
–40 bis 70 °C (–40 bis 158 °F)

Feuchtigkeitsbereich für den Betrieb:
10–90 % relative Feuchte

EMV-Leistungsdaten

Entspricht EN61326-1:2006.

Antennenoptionen

Integrierte Rundstrahlantenne
Optionale extern montierte Rundstrahlantenne

A.2 Geräteausführung

Gewicht

4,54 kg (10 lb.)

Werkstoffe

Gehäuse

Kupferarmes Aluminium, NEMA 4X

Lackierung

Polyurethan

Gehäusedeckeldichtung

Silikongummi

Antenne

Integrierte Antenne: PBT/PC

Externe Antenne: Glasfaser

Zertifikate

Class I Division 2 (USA)

Weltweit äquivalent

A.3 Kommunikationsspezifikationen

Galvanisch getrennter RS485

2-Leiter-Kommunikationsverbindung für Modbus RTU Multidrop-Anschlüsse

Baudrate: 57.600, 38.400, 19.200 oder 9.600

Protokoll: Modbus RTU

Verdrahtung: Einzeln abgeschirmt, paarweise verdrillt, 0,82 mm^2 (AWG 18). Verkabelungslänge ca. 1524 m (4000 ft.)

Ethernet

10/100base-TX Ethernet-Kommunikationsport
Protokolle: Modbus TCP, OPC, EtherNet/IP, HART-IP, https (für Web Interface)
Verdrahtung: Abgeschirmtes Cat5E-Kabel. Verkabelungslänge 100 m (328 ft.).

Modbus

Unterstützt Modbus RTU und Modbus TCP mit 32-Bit-Fließkommawerten, Ganzzahlen und skalierten Ganzzahlen.
Modbus Register sind benutzerdefiniert.

OPC

OPC Server unterstützt OPC DA v2, v3

EtherNet/IP

Unterstützt EtherNet/IP-Protokoll mit 32-Bit-Fließkommawerten und Ganzzahlen. EtherNet/IP Assembly Eingangs-/Ausgangsinstanzen sind vom Benutzer konfigurierbar.
EtherNet/IP-Spezifikationen werden von ODVA verwaltet und vertrieben.

A.4 Spezifikationen des selbstorganisierenden Netzwerks

Protokoll

IEC 62591 (WirelessHART), 2,4 bis 2,5 GHz DSSS.

Maximale Netzwerkgröße

100 Wireless-Geräte @ 8 Sekunden
50 Wireless-Geräte @ 4 Sekunden
25 Wireless-Geräte @ 2 Sekunden
12 Wireless-Geräte @ 1 Sekunden

Unterstützte Aktualisierungsraten der Geräte

Vom Anwender wählbar zwischen 1, 2, 4, 8, 16, 32 Sekunden oder 1 bis 60 Minuten

Netzwerkgröße/Latenz

100 Geräte: Weniger als 10 Sekunden
50 Geräte: Weniger als 5 Sekunden

Datenzuverlässigkeit

>99 %

A.5 Spezifikationen der Systemsicherheit

Ethernet

Aktiviert für (standardmäßige) Secure Sockets Layer (SSL) TCP/IP-Kommunikation

Zugriff auf das Smart Wireless Gateway

Aufgabenbasierte Zugriffsberechtigungen (RBAC) inkl. Administrator, Wartung, Bediener und Leitungspersonal. Der Administrator verfügt über die volle Kontrolle über das Gateway sowie die Verbindungen mit Hostsystemen und dem selbstorganisierenden Netzwerk.

Selbstorganisierendes Netzwerk

WirelessHART Protokoll mit Verschlüsselung gemäß AES-128, einschließlich individuellen Sitzungsschlüsseln. Bereitstellung von Geräten mittels Drag&Drop, einschließlich eindeutigem Verbindungsschlüssel und „weißer Liste".

Interne Firewall

Benutzerkonfigurierbare TCP-Ports für Kommunikationsprotokolle, einschließlich Aktivierung/Deaktivierung und benutzerdefinierter Portnummern. Überprüft sowohl eingehende als auch ausgehende Datenpakete.

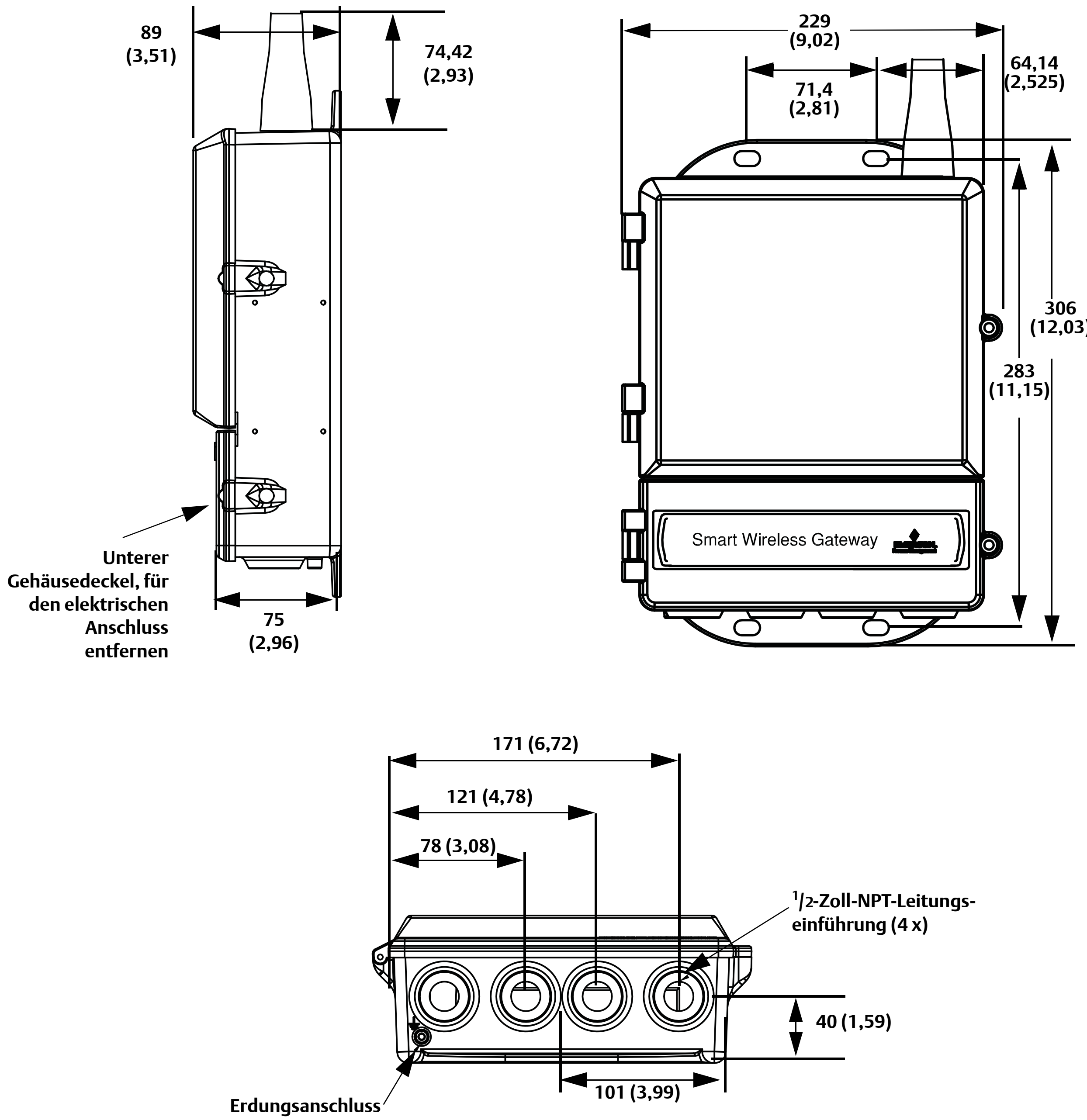
Zertifizierung von Fremdparteien

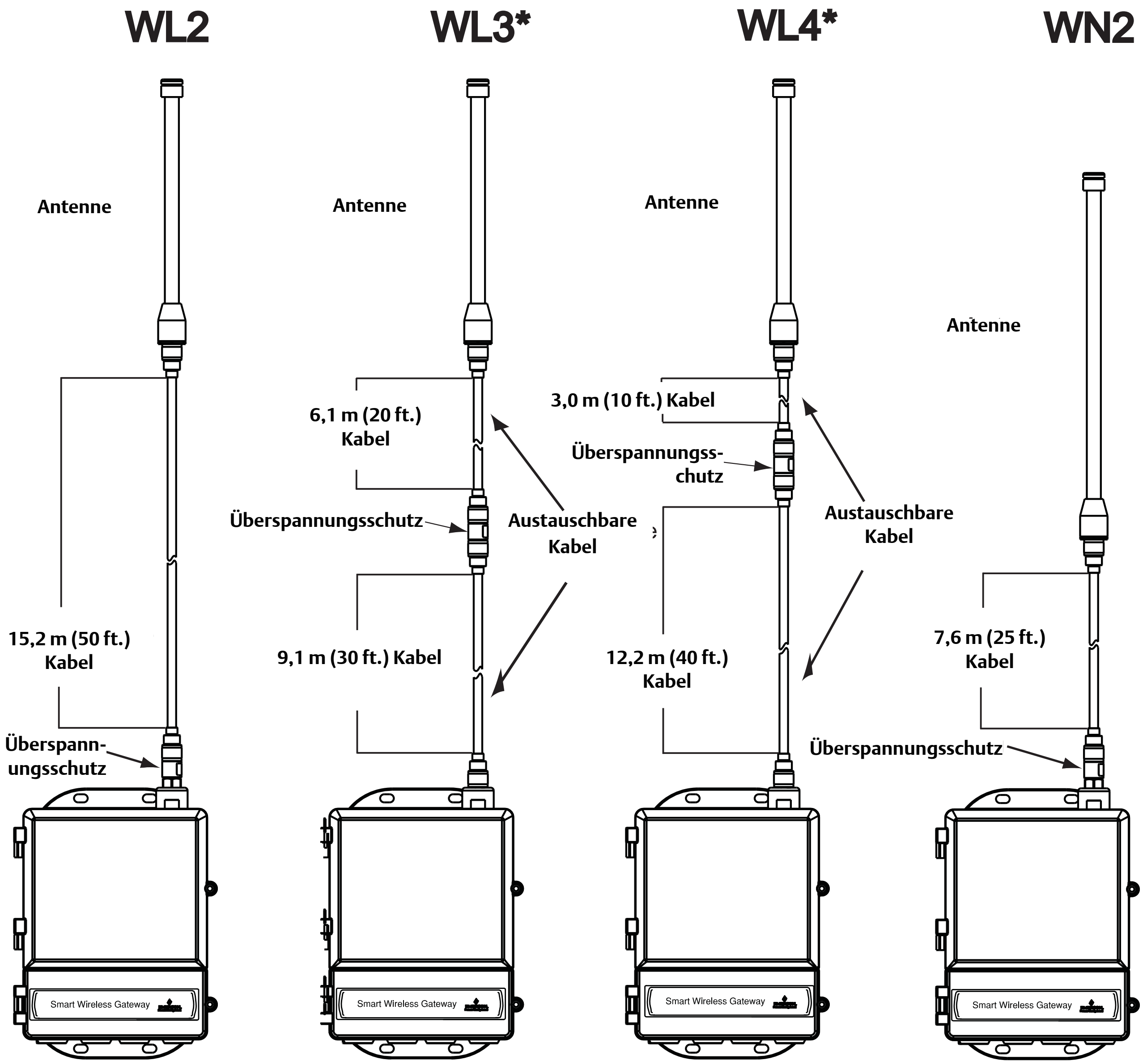
Wurldtech: Ausfallsicherheit des Netzwerks zertifiziert nach Achilles Level 1.

National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES)-Algorithmus gemäß Federal Information Processing Standard Publication 197 (FIPS-197).

A.6 Maßzeichnungen

Abbildung A-1. Smart Wireless Gateway (Abmessungen in mm [Zoll])





Externer Rundstrahlantennensatz

Der externe Rundstrahlantennensatz enthält ein Dichtungsband für den externen Antennenanschluss sowie Montagehalterungen für die Antenne, den Überspannungsschutz und das Smart Wireless Gateway.

Der Überspannungsschutz ist bei allen Optionen im Lieferumfang enthalten. WL3 und WL4 bieten einen Überspannungsschutz mit der Möglichkeit, das Gateway in Räumen, die Antenne im Freien und den Überspannungsschutz außerhalb des Gebäudes zu montieren.

Hinweis
Die Koaxialkabel der externen Antennenoptionen WL3 und WL4 sind zur leichteren Montage austauschbar.

A.7 Bestellinformationen

Tabelle A-1. Smart Wireless Gateway – Bestellinformationen

★ Die Standardausführung bietet die gebräuchlichsten Optionen. Die mit einem Stern (★) versehenen Optionen sollten ausgewählt werden, um die kürzeste Lieferzeit zu gewährleisten.
Für die erweiterten Produktangebote gelten längere Lieferzeiten.

Modell	Produktbeschreibung	
1420	Smart Wireless Gateway	
Spannungsversorgung		
Standard		**Standard**
A	24 VDC nominal (10,5–30 VDC)	★
Ethernet-Kommunikation – Physischer Anschluss		
Standard		**Standard**
1(1)(2)	Ethernet	★
2(3)(4)	Dual-Ethernet	★
Wireless Aktualisierungsrate, Betriebsfrequenz und Protokoll		
Standard		**Standard**
A3	Vom Anwender konfigurierbare Aktualisierungsrate, 2,4 GHz DSSS, *Wireless*HART	★
Serielle Kommunikation		
Standard		**Standard**
N	Keine	★
A(5)	Modbus RTU über RS485	★
Ethernet-Kommunikation – Datenprotokolle		
Standard		**Standard**
2	Webserver, Modbus TCP/IP, AMS Ready, HART-IP	★
4	Webserver, Modbus TCP/IP, AMS Ready, HART-IP, OPC	★
5(6)	DeltaV Ready	★
6(6)	Ovation Ready	★
8	Webserver, EtherNet/IP, AMS Ready, HART-IP	★
9	Webserver, EtherNet/IP, Modbus TCP/IP, AMS Ready, HART-IP	★

Optionen (mit der jeweiligen Modellnummer angeben)

Produkt-Zulassungen		
Standard		**Standard**
N5	FM Division 2, keine Funken erzeugend	★
N6	CSA Division 2, keine Funken erzeugend	★
N1	ATEX Typ n	★
ND	ATEX Staub	★
N7	IECEx Typ n	★
NF	IECEx Staub	★
KD	FM und CSA Division 2, keine Funken erzeugend und ATEX Typ n	★
N3	China Typ n	★
N4	TIIS Typ n	★
Redundanz-Optionen		
Standard		**Standard**
RD(7)(8)(9)	Gateway Redundanz	★

Tabelle A-1. Smart Wireless Gateway – Bestellinformationen

★ Die Standardausführung bietet die gebräuchlichsten Optionen. Die mit einem Stern (★) versehenen Optionen sollten ausgewählt werden, um die kürzeste Lieferzeit zu gewährleisten.
Für die erweiterten Produktangebote gelten längere Lieferzeiten.

Adapter		
Standard		**Standard**
J1	CM 20-Adapter für Leitungseinführung	★
J2	PG 13,5-Adapter für Leitungseinführung	★
J3	3/4 NPT-Adapter für Kabeleinführung	★
Antennenoptionen(10)		
Standard		**Standard**
WL2	Externer Antennensatz, 15,2 m (50 ft.) Kabel, Überspannungsschutz	★
WL3	Externer Antennensatz, 6,1 m (20 ft.) und 9,1 m (30 ft.) Kabel, Überspannungsschutz	★
WL4	Externer Antennensatz, 3,0 m (10 ft.) und 12,2 m (40 ft.) Kabel, Überspannungsschutz	★
Erweitert		
WN2(11)	Externer Hochleistungsantennensatz, 7,6 m (25 ft.) Kabel, Überspannungsschutz	
Typische Modellnummer: 1420 A 2 A3 A 2 N5		

(1) Ein aktiver 10/100 baseT-Ethernetport mit RJ45-Stecker.
(2) Zusätzliche Ports sind deaktiviert.
(3) Zwei aktive 10/100 baseT-Ethernetports mit RJ45-Steckern.
(4) Mehrere aktive Ports verfügen über separate IP-Adressen, Trennung durch Firewall und ohne Paketweiterleitung.
(5) Konvertierbar auf RS232 mittels Adapter, nicht im Lieferumfang des Gateway enthalten.
(6) Einschließlich Webserver, Modbus TCP, AMS Ready, HART-IP und OPC.
(7) Erfordert die Auswahl von Dual-Ethernet (Optionscode 2).
(8) Nicht lieferbar als DeltaV Ready (Optionscode 5).
(9) Nicht lieferbar mit den EtherNet/IP-Optionscodes 8 und 9
(10) Die Optionen WL2, WL3, WL4 und WN2 erfordern minimalen Montageaufwand.
(11) Nicht in allen Ländern verfügbar.

A.8 Zubehör und Ersatzteile

Tabelle A-2. Zubehör

Teilebeschreibung	Teilenummer
AMS Wireless SNAP-ON™, Lizenz für 1 Gateway	01420-1644-0001
AMS Wireless SNAP-ON, Lizenz für 5 Gateways	01420-1644-0002
AMS Wireless SNAP-ON, Lizenz für 10 Gateways	01420-1644-0003
AMS Wireless SNAP-ON, 5-10 Upgrade-Lizenzen	01420-1644-0004
Nur HART Modem und Kabel für seriellen Port	03095-5105-0001
Nur HART Modem und Kabel für USB-Port	03095-5105-0002

Tabelle A-3. Ersatzteile

Teilebeschreibung	Teilenummer
Ersatzteilsatz, WL2-Austausch(1), Externe Antenne, 15,2 m (50 ft.) Kabel, Überspannungsschutz	01420-1615-0302
Ersatzteilsatz, WL3-Austausch(1), Externe Antenne, 6,1/9,1 m (20/30 ft.) Kabel, Überspannungsschutz	01420-1615-0303
Ersatzteilsatz, WL4-Austausch(1), Externe Antenne, 3,0/12,2 m (10/40 ft.) Kabel, Überspannungsschutz	01420-1615-0304
Ersatzteilsatz, WN2-Austausch(1), Externer Hochleistungsantennensatz, 7,6 m (25 ft.) Kabel, Überspannungsschutz(2)	01420-1615-0402

(1) Kein Upgrade von integrierter auf externe Antenne möglich.
(2) Nicht in allen Ländern verfügbar.

Anhang B Produkt-Zulassungen

B.1 Zugelassene Herstellungsstandorte

Rosemount Inc. – Chanhassen, Minnesota, USA
Emerson Process Management GmbH & Co. OHG – Karlstein, Deutschland
Emerson Process Management Asia Pacific Private Limited – Singapur
Beijing Rosemount Far East Instrument Co., Limited – Peking, China

B.2 Übereinstimmung mit Telekommunikationsrichtlinien

Alle Wireless-Geräte müssen über Zertifikate verfügen, damit gewährleistet ist, dass sie die Richtlinien in Bezug auf die Verwendung des HF-Spektrums erfüllen. Für nahezu jedes Land ist eine solche Produktzertifizierung erforderlich. Emerson arbeitet mit Regierungsbehörden weltweit zusammen, damit seine Produkte vollständig mit diesen Richtlinien übereinstimmen und nicht gegen diese Richtlinien oder Gesetze, die die Verwendung von Wireless-Geräten regulieren, verstoßen.

B.3 FCC und IC

Dieses Gerät erfüllt Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden Bedingungen: Dieses Gerät darf keine schädliche Störstrahlung verursachen. Dieses Gerät muss Störsignale aufnehmen, auch solche, die zu Betriebsstörungen führen können. Dieses Gerät ist so zu installieren, dass der Mindestabstand zwischen Antenne und allen Personen 20 cm beträgt.

B.4 Standard-Bescheinigung nach FM

Das Gateway wurde standardmäßig von FM untersucht und geprüft, um zu gewährleisten, dass die Konstruktion die grundlegenden elektrischen, mechanischen und Brandschutzanforderungen erfüllt. FM ist ein national anerkanntes Prüflabor (NRTL), zugelassen von der Federal Occupational Safety and Health Administration (OSHA [US-Behörde für Sicherheit und Gesundheitsschutz am Arbeitsplatz]).

Nordamerikanische Zulassungen

N5 FM Division 2 (keine Funken erzeugend)
Zulassungs-Nr.: 3028321

Keine Funken erzeugend für Class I, Division 2, Groups A, B, C und D.
Geeignet für Class II, III, Division 2,
Groups E, F und G. Geschlossene Räume/im Freien.
Typ 4X
Temperaturcode: T4 (–40 °C ≤ T_a ≤ 60 °C)

Canadian Standards Association (CSA)

N6 CSA Division 2, keine Funken erzeugend
Zulassungs-Nr.: 1849337
Geeignet für Class I, Division 2, Groups A, B, C und D.
Installation gemäß Rosemount-Zeichnung 01420-1011.
Temperaturcode: T4 (–40 °C ≤ T_a ≤ 60 °C)
CSA-Gehäuseschutzart 4X

B.5 Informationen zu EU-Richtlinien

Die EU-Konformitätserklärung für alle auf dieses Produkt zutreffenden EU-Richtlinien ist auf der Rosemount Website unter www.rosemount.com zu finden. Diese Dokumente erhalten Sie auch durch Emerson Process Management.

ATEX-Richtlinie (94/9/EG)

Die Produkte von Emerson Process Management erfüllen die Anforderungen der ATEX-Richtlinie.

Elektromagnetische Verträglichkeit (EMV) (2004/108/EG)

Die Produkte von Emerson Process Management erfüllen die Anforderungen der EMV Richtlinie.

Europäische Richtlinie für Funkanlagen und Telekommunikationsendgeräte (R&TTE) (1999/5/EG)

Die Produkte von Emerson Process Management erfüllen die Anforderungen der R&TTE Richtlinie.

CE

Europäische Zulassungen

N1 ATEX Typ n
Zulassungs-Nr.: Baseefa 07ATEX0056X
ATEX-Kennzeichnung: Ex II 3 G
Ex nA nL IIC T4 (–40 °C ≤ T_a ≤ 60 °C)

Spezielle Voraussetzung zur sicheren Verwendung (X):

Der spezifische Oberflächenwiderstand der Antenne beträgt mehr als 1 Gigaohm. Um elektrostatische Aufladung zu verhindern, darf die Antenne nicht mit Lösungsmitteln oder trockenen Lappen abgerieben bzw. gereinigt werden.

Das Gerät besteht den 500-V-Isolationstest gemäß EN 60079-15:2005, Absatz 9.4 nicht. Dies muss bei der Montage berücksichtigt werden.

ND ATEX Staub
Zulassungs-Nr.: Baseefa 07ATEX0057
ATEX-Kennzeichnung: ⟨Ex⟩ II 3 D
Ex tD A 22 IP66 T135 (–40 °C ≤ T_a ≤ 60 °C)
Max. Betriebsspannung = 28 V

N7 IECEx Typ n
Zulassungs-Nr.: IECEx BAS 07.0012X
Ex nA nL IIC T4 (–40 °C ≤ T_a ≤ 60 °C)
Max. Betriebsspannung = 28 V

Spezielle Voraussetzung zur sicheren Verwendung (X):

Der spezifische Oberflächenwiderstand der Antenne beträgt mehr als 1 Gigaohm. Um elektrostatische Aufladung zu verhindern, darf die Antenne nicht mit Lösungsmitteln oder trockenen Lappen abgerieben bzw. gereinigt werden.

Das Gerät besteht den 500-V-Isolationstest gemäß EN 60079-15:2005, Absatz 9.4 nicht. Dies muss bei der Montage berücksichtigt werden.

NF IECEx Staub
Zulassungsnummer: IECEx BAS 07.0013
Ex tD A22 IP66 T135 (–40 °C ≤ T_a ≤ 60 °C)
Max. Betriebsspannung = 28 V

Zulassungskombinationen

KD Kombination von N5, N6 und N1.

Anhang C Delta V Ready

C.1 Übersicht

Die native Integration mit DeltaV ermöglicht die automatische Erkennung und die einfache Inbetriebnahme des Smart Wireless Gateway, um eine nahtlose Integration mit allen DeltaV Anwendungen zu gewährleisten: Explorer, Diagnostics und Control Studio. WirelessHART Geräte können dem Wireless-Feldnetzwerk auf einfache Weise hinzugefügt, über DeltaV Explorer abgestimmt und analogen Kanälen mittels Drag&Drop zugeordnet werden.

C.2 Latenzbetrachtungen für den Steuerlogikentwurf und -betrieb

Da die DeltaV Wireless I/O Scannersoftware jede Sekunde für 1/5 der Geräte Aktualisierungen anfordert, empfängt DeltaV für ein bestimmtes Feldgerät alle 5 Sekunden eine Aktualisierung. Dieser Empfang ist nicht unbedingt synchron mit der Aktualisierungsrate des Feldgerätes. Außerdem liegt zwischen der Messwertaufnahme eines Feldgerätes und der Weiterleitung in das Wireless Netzwerk eine Latenz. Auch Antworten auf Statusaktualisierungen können die Latenz in manchen Fällen erhöhen. Wenn also ein Gerät z. B. alle 8 Sekunden aktualisiert wird und die Latenz des Wireless Netzwerkes 2 Sekunden beträgt, kann die Zeitspanne zwischen dem Auftreten eines Ereignisses und der Verfügbarkeit auf dem DeltaV I/O Bus zwischen 0 und 15 (8+2+5) Sekunden betragen. Die Aktualisierungsperiode des DeltaV Regelmoduls sollte zu diesem Gesamtwert addiert werden, um den Latenzbereich für die Reaktion des Leitsystems auf ein Feldereignis zu bestimmen.

Die Bediener sollten darauf aufmerksam gemacht werden, dass die Aktualisierungsrate von Wireless Messungen auf Bedienermonitoren etwas langsamer ist als jene von verkabelten Geräten. Wenn der Bediener z. B. eine Ventilbewegung einleitet, kann es 5 bis 15 Sekunden dauern, bis eine Bestätigungsrückmeldung auf dem Bedienermonitor erscheint. Jede auf dieser Grundlage entworfene Steuerlogik sollte auch die Aktualisierungsraten und Latenzen berücksichtigen.

C.3 Anforderungen

DeltaV:

Version 10.3 oder neuer.

Smart Wireless Gateway:

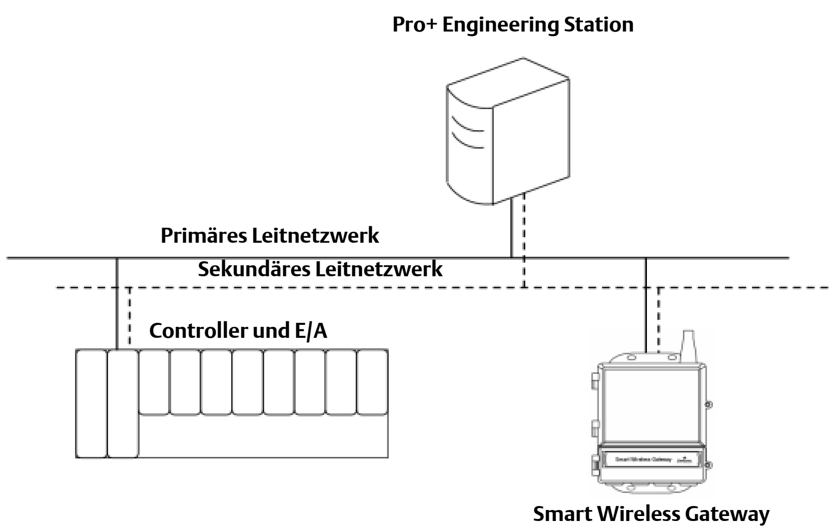
DeltaV Ready Option (Datenprotokoll-Option 5). Anhang A: Bestellinformationen

C.4 Montage und Anschluss

Das DeltaV Ready Gateway auf die gleiche Weise wie ein Standard Gateway montieren. (Abschnitt 3: Montage und Anschluss auf Seite 3-1). Das Gateway sollte an einem Ort installiert werden, an dem einfacher Zugriff auf das DeltaV Leitnetzwerk sowie das Wireless-Feldnetzwerk gegeben ist.

Den primären Ethernet-Port (Ethernet 1) des Gateway mit dem primären DeltaV Leitnetzwerk verbinden. Bei Bestellung des Gateway mit optionalem dualen Ethernet (physische Anschlussart Code 2) den sekundären Ethernet-Port (Ethernet 2) mit dem sekundären DeltaV Leitnetzwerk verbinden.

Abbildung C-1. Architektur des Delta V Leitnetzwerks



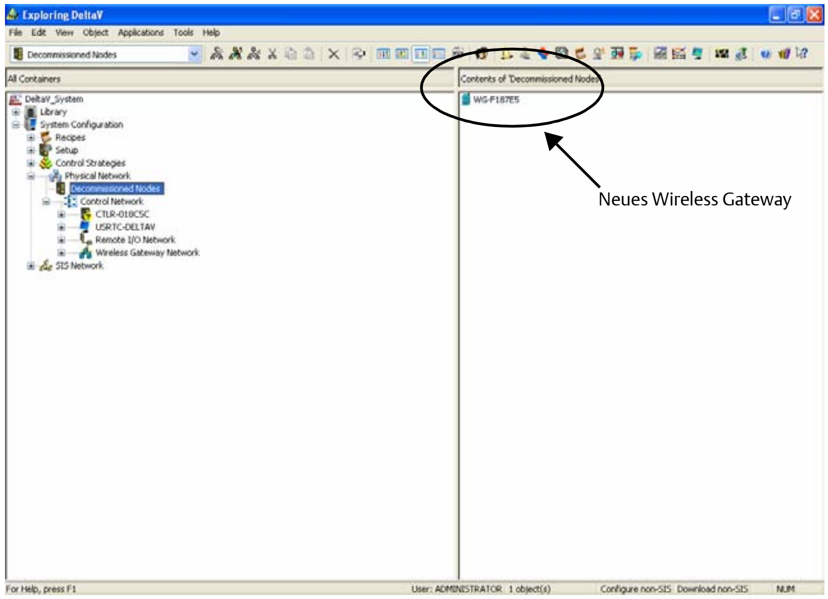
C.5 Einrichtung

Das Smart Wireless Gateway wird vorkonfiguriert für den Einsatz am DeltaV Leitnetzwerk geliefert. Das Gateway erscheint in der DeltaV Explore Anwendung automatisch im Ordner „Decommissioned Nodes“ (Außer Betrieb gesetzte Verbindungen).

Die Einrichtung eines Wireless-Netzwerks erfordert drei Schritte:

1. Inbetriebnahme des Gateway.
2. Zuordnung der Messstellenkennzeichnungen zu den Wireless-Geräten.
3. Zuordnung des Gateway zum Controller und Download.

Abbildung C-2. Ordner „Decommissioned Nodes“ (Außer Betrieb gesetzte Verbindungen) in Delta V Explorer



Inbetriebnehmen des Gateway:

1. Auf **START>PROGRAMS>DELTAV>ENGINEERING> DELTAV EXPLORE** klicken, um die DeltaV Explorer Anwendung zu starten.

2. Den Ordner **SYSTEM CONFIGURATION >PHYSICAL NETWORK>DECOMMISSIONED NODES** (Systemkonfiguration>Physisches Netzwerk>Außer Betrieb gesetzte Verbindungen) erweitern.

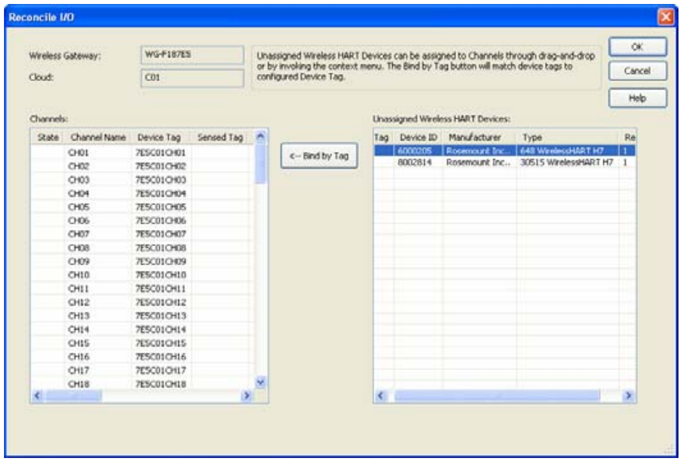
3. Mit der rechten Maustaste auf das *Smart Wireless Gateway* klicken und **Commission** (In Betrieb nehmen) auswählen.

4. Einen Namen für das Gateway eingeben und auf **OK** klicken.

5. Auf **YES** (Ja) klicken, wenn die Aufforderung *Auto-Sense Wireless Gateway* (Automatische Erkennung des Wireless Gateway) angezeigt wird.

An dieser Stelle wird das Fenster *Reconcile I/O* (E/A abstimmen) angezeigt. Dieser Bildschirm dient dem Zuordnen von WirelessHART Geräten zum DeltaV E/A-Kanal. Damit kann auch von anderen DeltaV Anwendungen wie Control Studio aus auf das Wireless-Gerät zugegriffen werden.

Abbildung C-3. Zuordnen von WirelessHART Geräten zum DeltaV E/A-Kanal



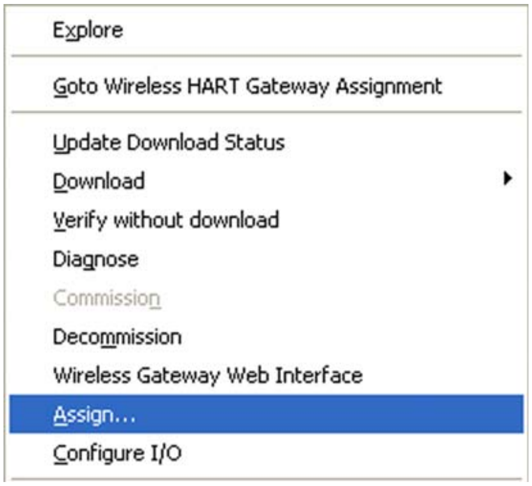
Zuweisen von Messstellenkennzeichnungen von Wireless-Geräten:

1. Das WirelessHART Gerät mittels Drag&Drop aus der Liste *Unassigned Wireless HART Devices:* (Nicht zugewiesene WirelessHART Geräte:) in die Liste *Channels:* (Kanäle:) ziehen.
2. Dieses Verfahren für jedes Wireless-Gerät wiederholen, bis alle Geräte zugewiesen wurden.
3. Auf **OK** klicken, um fortzufahren.

Anschließend muss das Gateway einem DeltaV Controller zugewiesen und alles heruntergeladen werden. Zuweisen und Herunterladen des Gateway:

1. Mit der rechten Maustaste auf das Gateway klicken und **Assign...** (Zuordnen) auswählen.
2. Den gewünschten Controller im Fenster „Browse“ (Durchsuchen) auswählen.
3. Auf **OK** klicken, um das Zuordnungsfenster zu schließen.
4. Mit der rechten Maustaste auf das Gateway klicken und **Download** auswählen.
5. Die Anweisungen im Download-Dialog befolgen.
6. Auf **OK** klicken, um das Download-Fenster zu schließen.

Abbildung C-4. Gateway Kontextmenü (Klick mit der rechten Maustaste).



Das Gateway und die Wireless-Geräte sind nun vollständig in Betrieb genommen und stehen auch anderen DeltaV Anwendungen zur Verfügung. Wenn dem Wireless-Netzwerk neue Geräte hinzugefügt werden, müssen diese den DeltaV Kanälen durch das Abstimmungsverfahren (mit der rechten Maustaste auf „Gateway“ klicken und „Configure IO“ [E/A konfigurieren]) zugewiesen werden.

Hinweis
Die Anmeldung beim Gateway unter Verwendung der standardmäßigen TCP/IP-Netzwerkeinstellung ist nicht möglich. Wenn das Gateway außer Betrieb genommen wurde, die IP-Adresse 10.5.255.254 verwenden. Wenn das Gateway in Betrieb ist, mit der rechten Maustaste in DeltaV Explore auf „Gateway“ klicken und „Wireless Gateway Web Interface“ auswählen.

Anhang D Redundanz

D.1 Übersicht

Ein redundantes Smart Wireless Gateway erhöht die Verfügbarkeit des Wireless-Feldnetzwerks durch Bereitstellung von zwei Sets physikalischer Hardware, die als ein einzelnes Gateway System betrieben werden. Dieser Abschnitt enthält Informationen über die Einrichtung und Installation eines redundanten Gateway Systems. Außerdem werden Diagnose und Integration behandelt, um die Überwachung des Zustands des redundanten Gateway Systems zu unterstützen.

- Montageort der jeweiligen Antennen
- Illustration der maximalen Redundanz einschl. Doppelschalter und USV
- Kenntnis der Störungsumschaltungsfunktion und zu erwartender Erfahrung
- Wirksamer Einsatz der Multimaster-Fähigkeit für Modbus Integrationen

D.2 Anforderungen

Smart Wireless Gateway:

Firmwareversion 4.3.19 oder höher, 4.4.15 wird empfohlen

Option RD für Gateway Redundanz

Statische IP-Adresse

Übereinstimmende Ausgangsprotokolle (z. B. Modbus oder OPC) an jedem Gateway

Hostsystem:

Ethernet-Verbindung für Modbus TCP oder OPC DA Kommunikation

Serielle Verbindung (RS-485) für Modbus RTU Kommunikation

D.3 Einrichtung

Bei der Konfiguration redundanter Smart Wireless Gateways muss nur eines der Systeme konfiguriert werden. Das andere Gateway wird automatisch konfiguriert, wenn es mit dem ersten Gateway „gepaart“ wird.

Ein Gateway auswählen, mit dem begonnen werden soll. Dieses Gateway wird im vorliegenden Dokument als Gateway A bezeichnet. Das andere Gateway ist Gateway B.

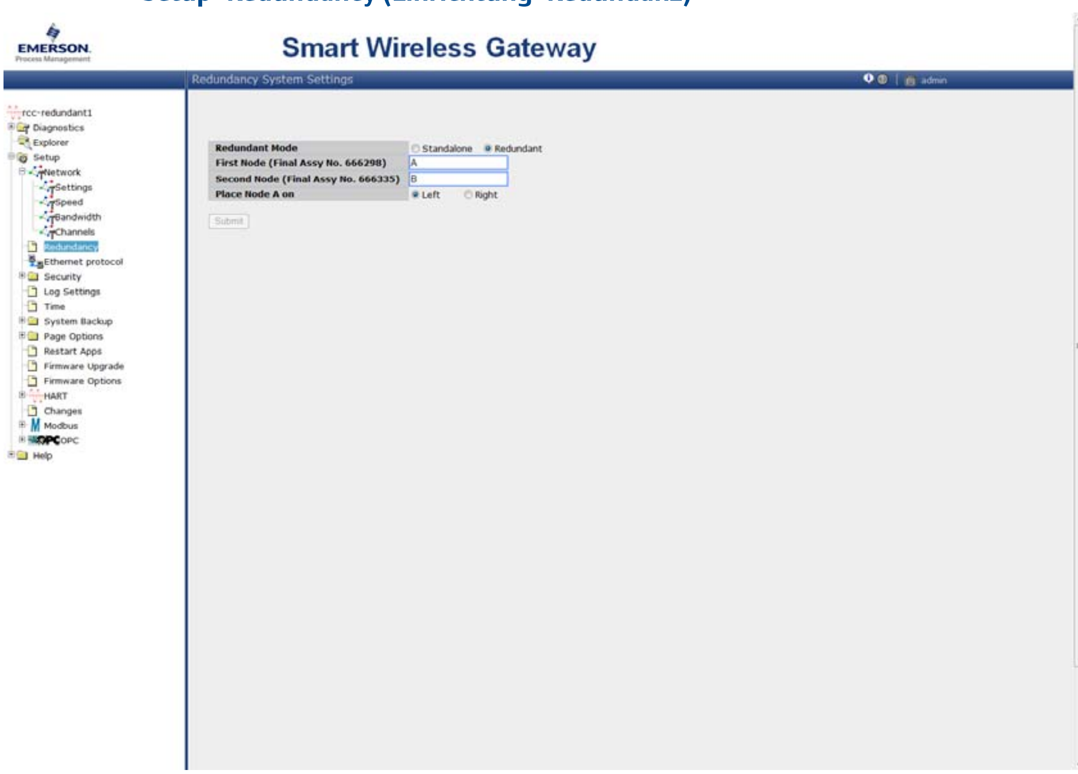
Konfigurieren der Einstellungen eines redundanten Systems:

1. Einen PC/Laptop an den Ethernet 1 Port von Gateway A anschließen.
2. Mit dem Benutzerkonto **admin** anmelden.
3. Zu **Setup>Redundancy** (Einrichtung > Redundanz) navigieren.
4. Einen benutzerdefinierten Namen für **First Node** (Erster Netzknoten), d. h. Gateway A, eingeben.
5. Einen benutzerdefinierten Namen für **Second Node** (Zweiter Netzknoten), d. h. Gateway B, eingeben.
6. Auswählen, ob Gateway A auf der **Linken** oder **Rechten** Seite montiert wird.
7. Auf **Submit** (Übertragen) klicken.

Die benutzerdefinierten Namen dienen zur Identifikation. Diese Namen werden in Diagnosemeldungen und bei der Integration in das Hostsystem verwendet, um die einzelnen Gateways identifizieren zu können. Es wird empfohlen, diese Namen nicht nur in den Konfigurationseinstellungen einzutragen, sondern auch auf den einzelnen Gateways zu kennzeichnen.

Für Visualierungszwecke auswählen, ob Gateway A auf der linken oder rechten Seite montiert wird. Dies hat keinen Einfluss auf die Leistungsmerkmale oder Funktionalität.

Abbildung D-1. Redundanz-Systemeinstellungen
Setup>Redundancy (Einrichtung>Redundanz)

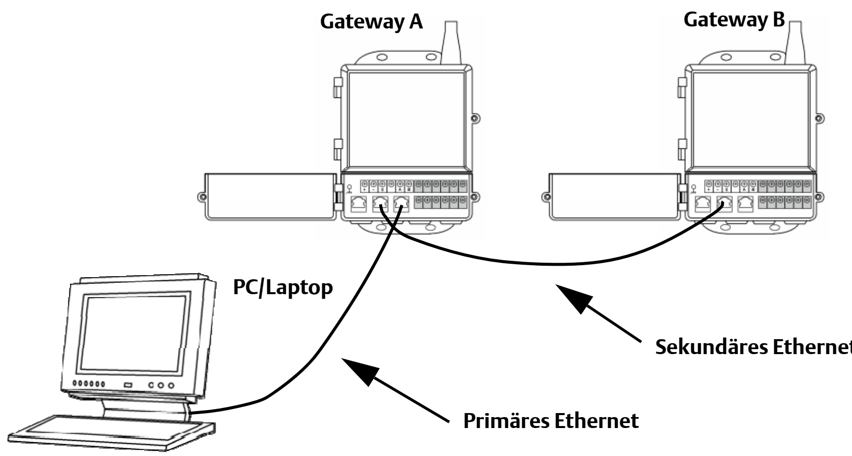


Nachdem die Einstellungen des redundanten Systems konfiguriert wurden, müssen die beiden Gateways verbunden und als Paar festgelegt werden.

Paaren zweier Gateways, um ein redundantes System zu bilden:

1. Einen PC/Laptop an den primären Ethernet-Port von Gateway A anschließen.
2. Mit dem Benutzerkonto **admin** anmelden.
3. Zu **Diagnostics>Advanced>Redundancy Status** (Diagnose > Erweitert > Redundanzstatus) navigieren.
4. Den sekundären Ethernet-Port von Gateway A mit dem sekundären Ethernet-Port von Gateway B (siehe Abbildung D-2 auf Seite 75, Einrichtung der Redundanz-Verbindungen) verbinden.
5. Auf dem erscheinenden Dialogfeld auf **Form redundant pair** (Redundantes Paar bilden) klicken.
6. Warten, bis der Status **Pairing to redundant peer** (Paarung mit redundantem System) **grün** angezeigt wird.
7. Auf **Return to page** (Zurück zur Seite) klicken.

Abbildung D-2. Einrichtung der Redundanz-Verbindungen



Nachdem die Gateways „gepaart“ wurden, wird Gateway A als derzeit aktives Gateway auf der linken Seite und Gateway B als Standby-Gateway auf der rechten Seite angezeigt (die Anordnung links oder rechts kann auf der Seite „Redundancy System Settings“ [Einstellungen des redundanten Systems] geändert werden). Wenn umfangreiche Konfigurationsänderungen auf das Standby-Gateway heruntergeladen werden müssen, kann dieses kurz nach Abschluss des Paarungsverfahrens kurzzeitig offline gehen. Dies ist normal und stellt keine Instabilität des Systems dar.

D.4 Montage und Anschluss

Redundante Gateways werden auf ähnliche Weise wie das eigenständige Gateway montiert und angeschlossen. Weitere Informationen sind in Abschnitt 3: Montage und Anschluss zu finden. Zusätzlich zu den Standardverfahren sind die folgenden Hinweise bei der Installation redundanter Gateways zu berücksichtigen.

Montage

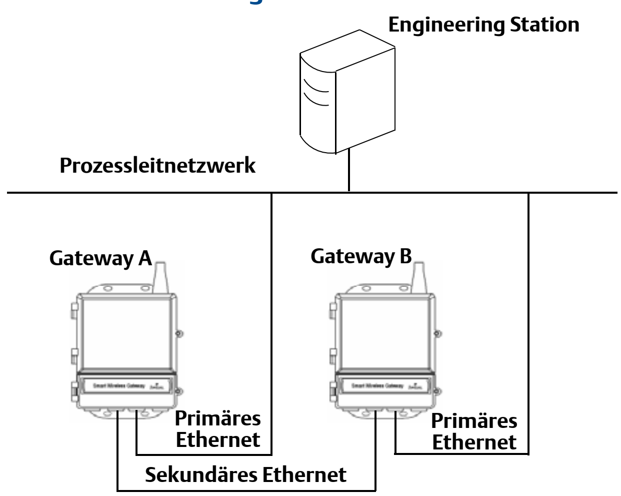
Die redundanten Gateways sollten an einem Ort installiert werden, an dem einfacher Zugriff auf das Leitnetzwerk sowie eine gute Abdeckung für das Wireless-Feldnetzwerk gegeben ist.

Die Antennen der redundanten Gateways sollten auf gleicher Höhe und mit einem horizontalen Abstand von 1 m bis 3 m (3 ft. bis 9 ft.) montiert werden. Dies soll gewährleisten, dass eine identische Abdeckung für das Wireless-Feldnetzwerk gegeben ist und dass im Falle einer Umschaltung Abdeckungslücken eliminiert werden.

Ethernet

Eine Ethernet-Verbindung mit dem Hostsystem unterstützt Modbus TCP, OPC, AMS Wireless Configurator und HART IP Protokolle. Bei Verwendung dieser Architektur den sekundären Ethernet-Port von Gateway A direkt mit dem sekundären Ethernet-Port von Gateway B verbinden. Anschließend den primären Ethernet-Port beider Gateways mittels separater/redundanter Netzwerkschalter mit einem Leitnetzwerk verbinden. Siehe Abbildung D-3 Ethernet-Verbindungsarchitektur.

Abbildung D-3. Ethernet-Verbindungsarchitektur

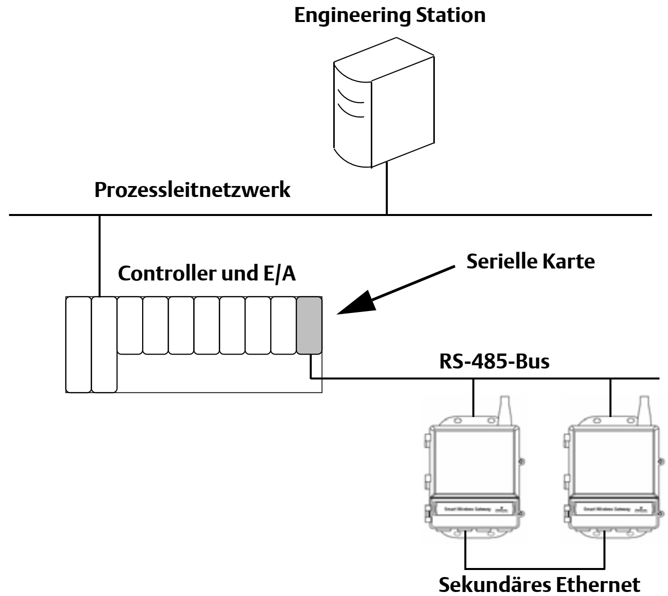


Hinweis
Der primäre Ethernet-Port jedes Gateway sollte mit separaten Netzwerkschaltern am gleichen Leitnetzwerk verbunden werden. Einzelheiten über verfügbare redundante Netzwerkschalter erhalten Sie vom Administrator des Leitnetzwerks.

Simplex RS-485

Eine RS-485 Simplex Verbindung mit einem Host unterstützt das Modbus RTU Protokoll. Bei Verwendung dieser Architektur den sekundären Ethernet-Port von Gateway A direkt mit dem sekundären Ethernet-Port von Gateway B verbinden. Anschließend die RS-485-Ports beider Gateways parallel mit einer seriellen Karte am Hostsystem verdrahten. Siehe Abbildung D-4 Simplex RS-485-Architektur.

Abbildung D-4. Simplex RS-485-Architektur

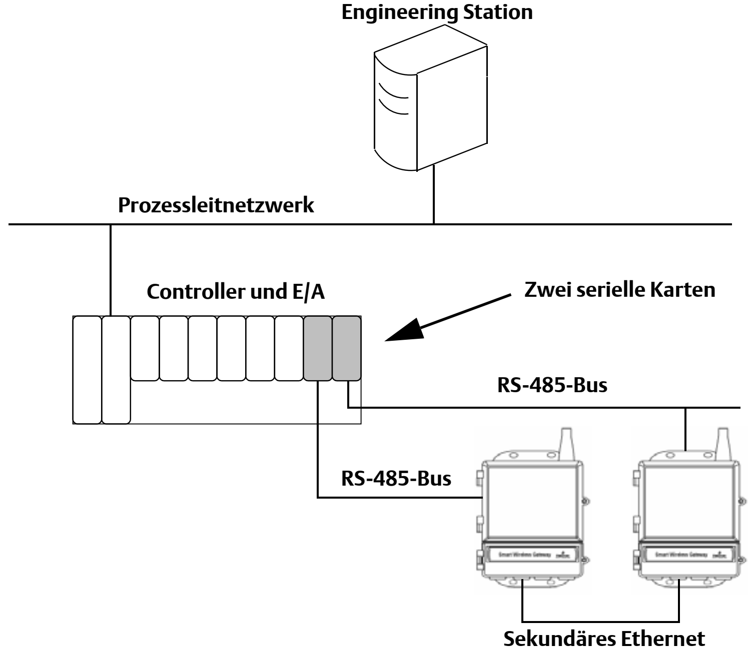


Hinweis
Sowohl in der Simplex- als auch in der dualen RS-485-Architektur können die primären Ethernet-Ports mit einem Asset-Management-Netzwerk verbunden werden, um die Konnektivität mit AMS Device Manager oder AMS Wireless Configurator zu ermöglichen.

Duale RS-485

Eine RS-485-Dual-Verbindung mit einem Host unterstützt das Modbus RTU Protokoll. Bei Verwendung dieser Architektur den sekundären Ethernet-Port von Gateway A direkt mit dem sekundären Ethernet-Port von Gateway B verbinden. Anschließend die RS-485-Ports beider Gateways separat mit den zwei seriellen Karten am Hostsystem verdrahten. Siehe Abbildung D-5 Duale RS-485-Architektur.

Abbildung D-5. Duale RS-485-Architektur



Hinweis
In einem redundanten System werden Modbus Abfrageanforderungen standardmäßig nur vom aktiven Gateway beantwortet. Wenn beide Gateways abgefragt werden sollen, beim Gateway Web Interface anmelden, zu „Setup>Modbus>Communications“ (Einrichtung>Modbus> Kommunikation) navigieren und „Respond when running as redundant standby?“ (Reagiert redundantes Standby-Gateway auf Abfragen?) auf „Yes“ (Ja) setzen. Diese Einstellung ausschließlich in einer dualen RS-485-Architektur verwenden.

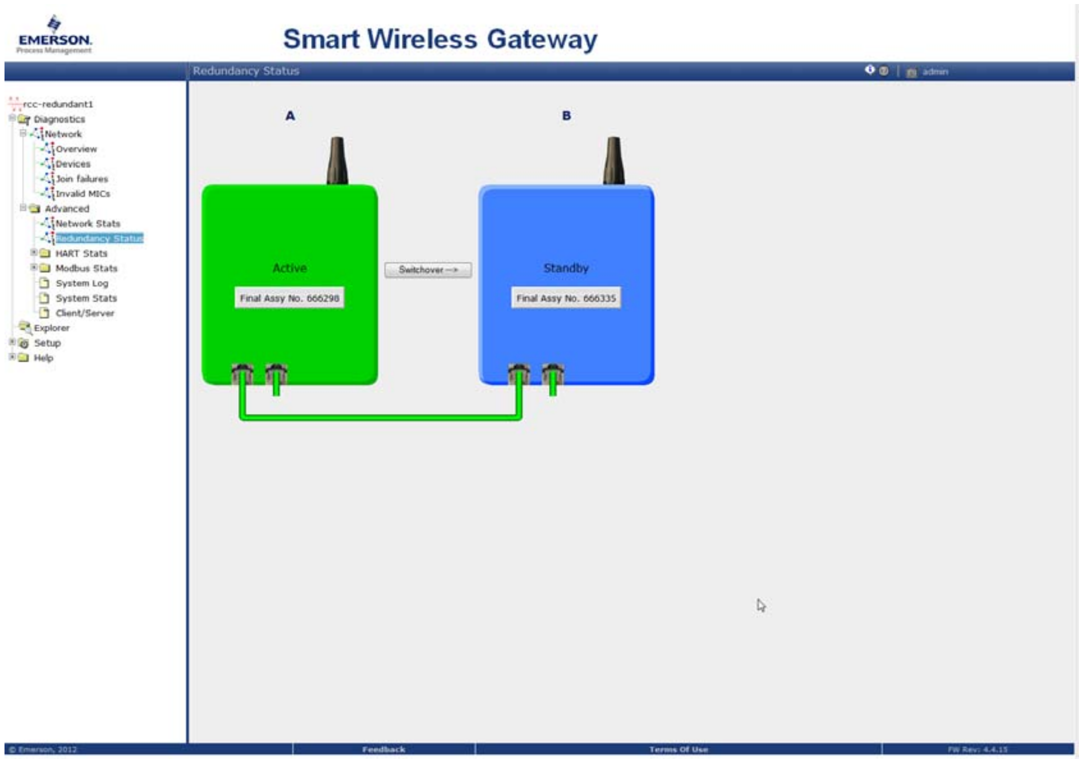
Spannungsversorgung

Die Spannungsversorgung der redundanten Gateways sollte erst dann eingeschaltet werden, nachdem alle primären und sekundären Ethernet- und RS-485-Verbindungen hergestellt wurden. Es wird empfohlen, separate unterbrechungsfreie Stromversorgungen (USV) zu verwenden, um die Verfügbarkeit des redundanten Gateway Systems bei einem Spannungsausfall zu gewährleisten.

D.5 Diagnose

Das redundante System führt zahlreiche Diagnoseprüfungen durch, um den Zustand und die Konnektivität des Systems zu verifizieren. Diese Diagnoseinformationen sind unter **Diagnostics>Advanced>Redundancy Status** (Diagnose > Erweitert > Redundanzstatus) zu finden.

Abbildung D-6. Redundanzstatus Diagnostics>Advanced>Redundancy Status (Diagnose > Erweitert > Redundanzstatus)



Die Diagnoseinformationen können außerdem Modbus-Registern oder OPC Kennzeichnungen zugeordnet werden. Die folgende Tabelle zeigt, welche Diagnoseinformationen auf der Seite „Redundancy Status“ (Redundanzstatus) zu finden sind und wie diese in Modbus oder OPC als Parameter zugeordnet werden können.

Tabelle D-1. Redundanzstatus-Diagnoseinformationen

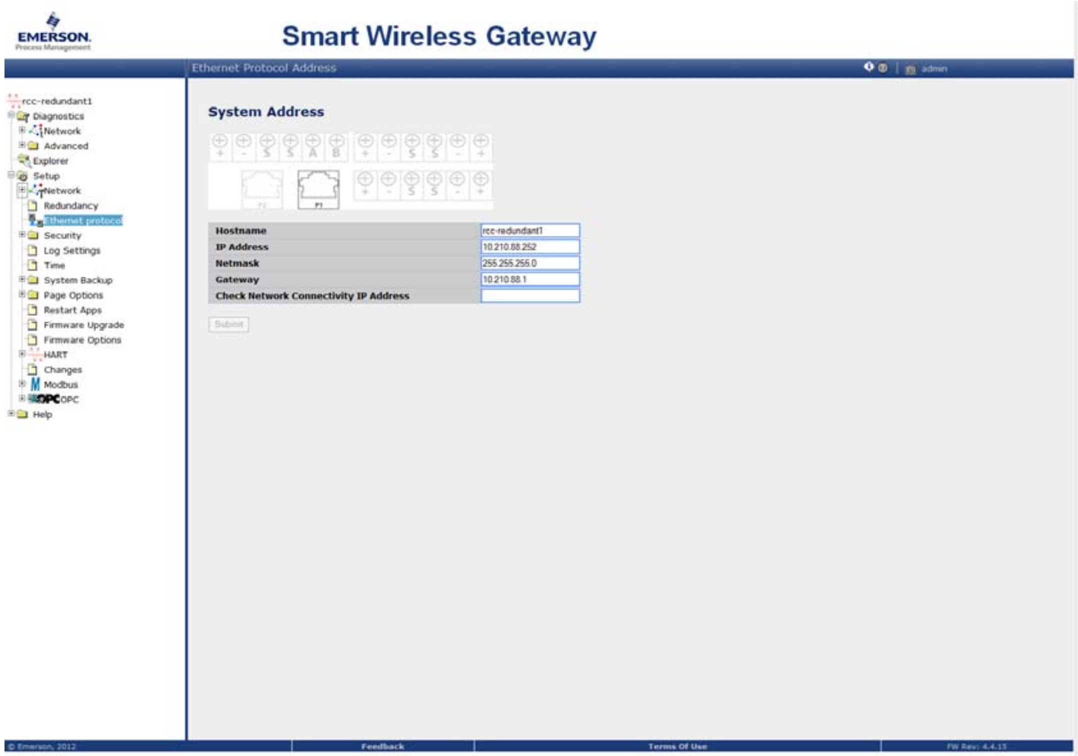
Parameter	Beschreibung	Datentyp
REDUNDANT_HEALTHY	Allgemeiner Redundanzstatus, der angibt, ob das System zum Umschalten bereit ist	Boolean
RF_COVERAGE_FAILURE	Prüfen, ob beide Gateways die gleiche HF-Abdeckung des Wireless-Feldnetzwerks gewährleisten	Boolean
REDUNDANT_A_ONLINE	Betriebsstatus von Gateway A	Boolean
REDUNDANT_A_MASTER	Gibt an, ob Gateway A das aktive System ist	Boolean
REDUNDANT_A_PING	Gibt an, ob Gateway A die festgelegte IP-Adresse eines Hostsystems erreichen kann	Boolean
REDUNDANT_A_ETH0	Status der elektrischen Verbindung des primären Ethernet-Ports von Gateway A	8-Bit-Ganzzahl ohne Vorzeichen
REDUNDANT_B_ONLINE	Betriebsstatus von Gateway B	Boolean
REDUNDANT_B_MASTER	Gibt an, ob Gateway B das aktive System ist	Boolean
REDUNDANT_B_PING	Gibt an, ob Gateway B die festgelegte IP-Adresse eines Hostsystems erreichen kann	Boolean
REDUNDANT_B_ETH0	Status der elektrischen Verbindung des primären Ethernet-Ports von Gateway A	8-Bit-Ganzzahl ohne Vorzeichen

Neben den Redundanzstatus-Diagnoseinformationen kann eine zusätzliche Prüfung konfiguriert werden, um die Konnektivität des Netzwerks mit einem Hostsystem oder einer anderen Anwendung zu testen. Das redundante System verwendet diese Prüfung, um die beste Verbindungsmöglichkeit zu bestimmen und festzulegen, welches Gateway als aktives Gateway verwendet werden sollte.

Konfigurieren der Netzwerk-Verbindungsprüfung:

1. Zu **Setup**>**Ethernet Protocol** (Einrichtung>Ethernet-Protokoll) navigieren.
2. Die IP-Adresse des Hostsystems in das Feld *Check Network Connectivity IP Address* (IP-Adresse für Netzwerkverbindung prüfen) eingeben.
3. Auf **Submit** (Übertragen) klicken.

Abbildung D-7. Network Connectivity Check Setup>Network>Ethernet protocol (Einrichtung>Netzwerk>Ethernetprotokoll)



D.6 Austausch eines Gateway

Beim Austausch oder beim Wiedereinbau eines Gateway in ein redundantes System muss stets die primäre und sekundäre Ethernet-Verbindung hergestellt werden, bevor die Spannungsversorgung des Standby Gateway eingeschaltet wird. Wenn das Gateway wieder eingebaut wird (d. h. es war Teil des originalen redundanten Systems), wird es automatisch wieder in das redundante System aufgenommen. Wenn das Gateway neu ist oder auf die Standardkonfiguration gesetzt wurde, muss es mit dem derzeit aktiven Gateway „gepaart“ werden. Zu „Diagnostics>Advanced>Redundancy Status“ (Diagnose>Erweitert>Redundanzstatus) navigieren und die empfohlenen Maßnahmen auf dieser Seite oder das obige Verfahren zum „Paaren“ von Gateways befolgen, um ein redundantes System zu bilden.

Deutschland
Emerson Process Management GmbH & Co. OHG
Argelsrieder Feld 3
82234 Weßling
Deutschland
T +49 (0) 8153 939 - 0
F +49 (0) 8153 939 - 172
www.emersonprocess.de

Schweiz
Emerson Process Management AG
Blegistrasse 21
6341 Baar-Walterswil
Schweiz
T +41 (0) 41 768 6111
F +41 (0) 41 761 8740
www.emersonprocess.ch

Österreich
Emerson Process Management AG
Industriezentrum NÖ Süd
Straße 2a, Objekt M29
2351 Wr. Neudorf
Österreich
T +43 (0) 2236-607
F +43 (0) 2236-607 44
www.emersonprocess.at